One Identity Manager 9.1.1

Administrationshandbuch für das Identity Management Basismodul

Legende

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

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

One Identity Manager Administrationshandbuch für das Identity Management Basismodul
Aktualisiert - 28. März 2023, 21:24 Uhr

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

Inhalt

Grundlagen zur Abbildung von Unternehmensstrukturen im One Identity Manager

Mit dem One Identity Manager können die Personen in einem Unternehmen entsprechend ihrer Funktion mit Unternehmensressourcen, beispielsweise Berechtigungen oder Software, versorgt werden. Dafür werden im One Identity Manager die Unternehmensstrukturen in Form hierarchisch aufgebauter Rollen dargestellt.

Rollen sind Objekte über die Unternehmensressourcen zugewiesen werden können. Dazu werden Personen, Geräte und Arbeitsplätze den Rollen als Mitglieder zugeordnet. Bei entsprechender Konfiguration des One Identity Manager erhalten die Mitglieder über diese Rollen ihre Unternehmensressourcen.

Zuweisungen von Unternehmensressourcen werden somit nicht mehr zu jeder einzelnen Person, jedem Gerät oder jedem Arbeitsplatz vorgenommen, sondern an einer zentralen Stelle und dann automatisch an vorher definierte Verteiler vererbt.

Im One Identity Manager sind folgende Rollen zur Abbildung von Unternehmensstrukturen definiert:

- Abteilungen, Kostenstellen und Standorte

  Aufgrund ihrer besonderen Bedeutung für betriebliche Abläufe in vielen Unternehmen werden Abteilungen, Kostenstellen und Standorte in eigenständigen Hierarchien, unter dem Begriff **Organisationen** abgebildet.

- Geschäftsrollen

  Geschäftsrollen bilden Unternehmensstrukturen mit gleichartiger Funktionalität ab, die zusätzlich zu Abteilungen, Kostenstellen und Standorten existieren. Das können zum Beispiel Projektgruppen sein. Ausführliche Informationen zu Geschäftsrollen finden Sie im *One Identity Manager Administrationshandbuch für Geschäftsrollen*.

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

- Anwendungsrollen

  Anwendungsrollen werden genutzt, um Berechtigungen auf die One Identity Manager Objekte an die One Identity Manager Benutzer zu vergeben. Ausführliche

Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Detaillierte Informationen zum Thema

- Grundlagen für den Aufbau von hierarchischen Rollen auf Seite 11
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Grundlagen zur Berechnung der Vererbung auf Seite 21
- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 25

Grundlagen für den Aufbau von hierarchischen Rollen

Abteilungen, Kostenstellen, Standorte und Anwendungsrollen werden hierarchisch angeordnet. Über diese Hierarchien werden die zugeordneten Unternehmensressourcen an ihre Mitglieder vererbt. Zuweisungen von Unternehmensressourcen werden somit nicht mehr zu jeder einzelnen Person, jedem Gerät oder jedem Arbeitsplatz vorgenommen, sondern an einer zentralen Stelle und dann automatisch an vorher definierte Verteiler vererbt.

Die Erstellung von Hierarchien kann im One Identity Manager entweder nach dem Top-Down-Modell oder Bottom-Up-Modell erfolgen. Beim Top-Down-Modell werden Rollen anhand von Aufgabengebieten definiert und die zur Erfüllung der Aufgaben benötigten Unternehmensressourcen den Rollen zugeordnet. Beim Bottom-Up-Modell werden die zugeordneten Unternehmensressourcen analysiert und daraus Rollen abgeleitet.

Detaillierte Informationen zum Thema

- Vererbungsrichtungen innerhalb einer Hierarchie auf Seite 12
- Unterbrechen der Vererbung auf Seite 14

Vererbungsrichtungen innerhalb einer Hierarchie

Innerhalb einer Hierarchie entscheidet die Vererbungsrichtung über die Zuteilung der Unternehmensressourcen. Grundsätzlich kennt der One Identity Manager zwei Vererbungsrichtungen:

- Top-Down-Vererbung

  Die Standardstruktur innerhalb eines Unternehmens wird im One Identity Manager über die Top-Down-Vererbung realisiert. Mit ihrer Hilfe wird beispielsweise die mehrstufige Gliederung eines Unternehmens in Hauptabteilungen und darunter liegende Fachabteilungen abgebildet.

- Bottom-Up-Vererbung

  Während mit der Top-Down-Vererbung die Zuweisungen in Richtung der feineren Gliederung vererbt werden, wirkt die Bottom-Up-Vererbung in umgekehrter Richtung. Diese Vererbungsrichtung wurde besonders im Hinblick auf die Abbildung von Projektgruppen eingeführt. Das Ziel ist dabei, dem Koordinator mehrerer Projektgruppen die Unternehmensressourcen, mit denen die einzelnen Projektgruppen umgehen, zur Verfügung zu stellen.

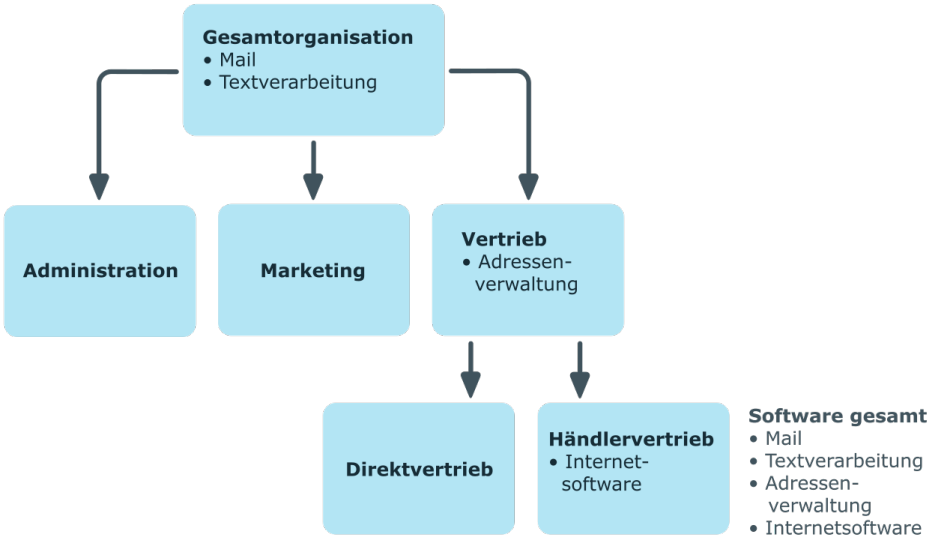
HINWEIS: Die Vererbungsrichtung wird nur bei der Vererbung von Unternehmensressourcen beachtet. Auf die Ermittlung der verantwortlichen Manager hat die Vererbungsrichtung keinen Einfluss. Der Manager einer übergeordneten Rolle ist immer für alle untergeordneten Rollen verantwortlich.

Die Auswirkungen auf die Zuteilung der Unternehmensressourcen werden nachfolgend am Beispiel der Applikationszuweisung erläutert.

Beispiel: Zuweisung von Unternehmensressourcen über Top-Down-Vererbung

Es wird ein Ausschnitt aus einer Unternehmensstruktur dargestellt. Zusätzlich sind Software-Anwendungen aufgeführt, die der jeweiligen Abteilung zugewiesen sind. Eine Person des Händlervertriebes erhält alle Software-Anwendungen, die ihrer Abteilung und allen Abteilungen auf dem Pfad zur Gesamtorganisation zugewiesen sind. In diesem Fall sind das Mail, Textverarbeitung, Adressenverwaltung und Internetsoftware.

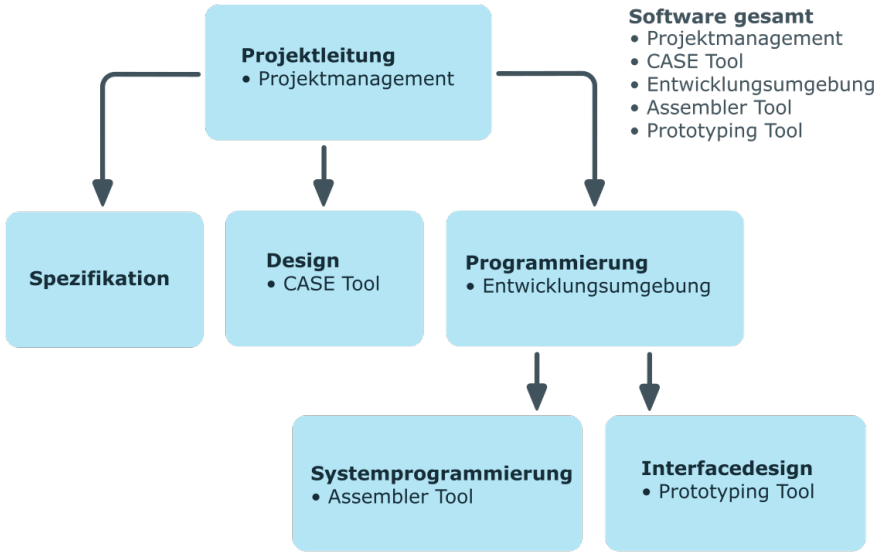
Abbildung 1: Zuweisung über Top-Down-Vererbung



Beispiel: Zuweisung von Unternehmensressourcen über Bottom-Up-Vererbung

In der nachfolgenden Abbildung ist eine Bottom-Up-Vererbung im Rahmen eines Projektes angedeutet. Zusätzlich sind Software-Anwendungen aufgeführt, die der jeweiligen Projektgruppe zugewiesen sind. Eine Person der Projektgruppe "Projektleitung" erhält neben den Software-Anwendungen ihrer Projektgruppe alle Software-Anwendungen der ihr unterstellten Projektgruppen. In diesem Fall sind das Projektmanagement, CASE Tool, Entwicklungsumgebung, Assembler Tool und Prototyping Tool.

Abbildung 2: Zuweisung über Bottom-Up-Vererbung



Unterbrechen der Vererbung

In speziellen Fällen ist die Vererbung über mehrere Hierarchieebenen nicht gewünscht. Deshalb ist die Unterbrechung der Vererbung innerhalb einer Hierarchie möglich. An welcher Stelle der Hierarchie die Vererbung unterbrochen wird, wird mit der Option **Vererbung blockieren** festgelegt. In Abhängigkeit von der gewählten Vererbungsrichtung hat diese Festlegung unterschiedliche Auswirkungen.

- Bei einer Top-Down-Vererbung erbt die mit der Option **Vererbung blockieren** versehene Rolle keine Zuweisungen aus der übergeordneten Ebene. Sie vererbt die ihr direkt zugewiesenen Unternehmensressourcen ihrerseits jedoch an die ihr untergeordneten Ebenen weiter.
- In einer Bottom-Up-Vererbung erbt die mit der Option Vererbung blockieren versehene Rolle alle Zuweisungen der untergeordneten Ebenen. Die Rolle selbst vererbt jedoch keinerlei Zuweisungen weiter nach oben.

Die Option **Vererbung blockieren** hat keinen Einfluss auf die Berechnung der verantwortlichen Manager.

Beispiel: Unterbrechung der Vererbung in einer Top-Down-Vererbung

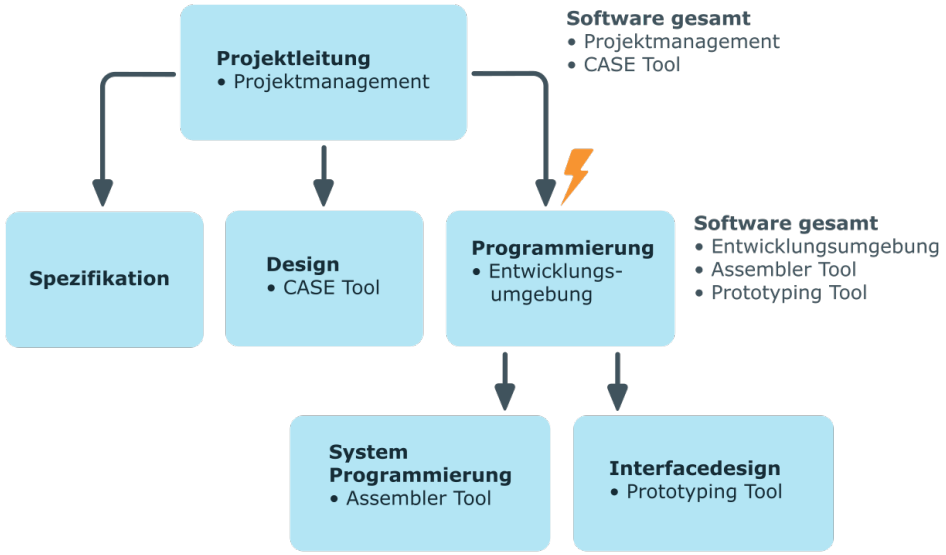
Wird im Beispiel einer Top-Down-Vererbung für die Abteilung "Vertrieb" die Option **Vererbung blockieren** gesetzt, hat das zur Folge, dass eine Person in der Abteilung "Vertrieb" nur die Software "Adressenverwaltung" und eine Person in der Abteilung "Händlervertrieb" die Software "Adressenverwaltung" und "Internetsoftware" erbt. Die Software-Anwendungen der Abteilung "Gesamtorganisation" werden jedoch nicht an die Personen in den Abteilungen "Vertrieb" und "Händlervertrieb" zugewiesen.

Abbildung 3: Unterbrechung der Vererbung in einer Top-Down-Vererbung

Beispiel: Unterbrechung der Vererbung in einer Bottom-Up-Vererbung

Eine Person der Projektgruppe "Programmierung" erhält neben den Software-Anwendungen seiner Projektgruppe alle Software-Anwendungen der ihr unterstellten Projektgruppen. In diesem Fall die Entwicklungsumgebung, Assembler Tool und Prototyping Tool. Wird die Projektgruppe "Programmierung" mit der Option **Vererbung blockieren** versehen, vererbt sie keine Zuweisungen weiter. In der Folge wird den Personen in der Projektgruppe "Projektleitung" neben der Software-Anwendung Projektmanagement nur das CASE Tool zugewiesen. Die Software-Anwendungen der Projektgruppen "Programmierung", "Systemprogrammierung" und "Interfacedesign" werden nicht an die Projektleitung vererbt.

Abbildung 4: Unterbrechung der Vererbung in einer Bottom-Up-Vererbung



Verwandte Themen

- Vererbung über Rollen blockieren auf Seite 32

Grundlagen zur Zuweisung von Unternehmensressourcen

Unternehmensressourcen können im One Identity Manager an Personen, Geräte und Arbeitsplätze zugewiesen werden. Bei Zuweisung von Unternehmensressourcen werden unterschiedliche Zuweisungsarten genutzt.

Die Zuweisungsarten sind:

- Direkte Zuweisung von Unternehmensressourcen
- Indirekte Zuweisung von Unternehmensressourcen
- Zuweisung von Unternehmensressourcen über dynamische Rollen
- Zuweisung von Unternehmensressourcen über IT Shop Bestellungen

Direkte Zuweisung von Unternehmensressourcen

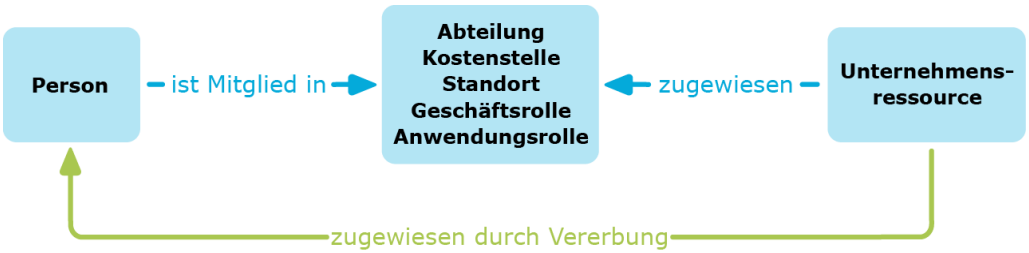
Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Person, einem Gerät oder einem Arbeitsplatz. Durch die direkte Zuweisung von Unternehmensressourcen kann ohne weiteren Aufwand auf Sonderanforderungen reagiert werden.

Abbildung 5: Schema einer direkten Zuweisung am Beispiel Person

Indirekte Zuweisung von Unternehmensressourcen

Bei der indirekten Zuweisung von Unternehmensressourcen werden Personen, Geräte und Arbeitsplätze in Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Anwendungsrollen eingeordnet. Aus der Position innerhalb der Hierarchie, der Vererbungsrichtung (Top-Down, Bottom-Up) und den Unternehmensressourcen, die diesen Rollen zugeordnet sind, berechnet sich die Summe der zugeordneten Unternehmensressourcen für eine Person, ein Gerät oder einen Arbeitsplatz. Bei der indirekten Zuweisung von Unternehmensressourcen wird nochmals zwischen der primären Zuweisung und der sekundären Zuweisung unterschieden.

Abbildung 6: Schema einer indirekten Zuweisung am Beispiel Person



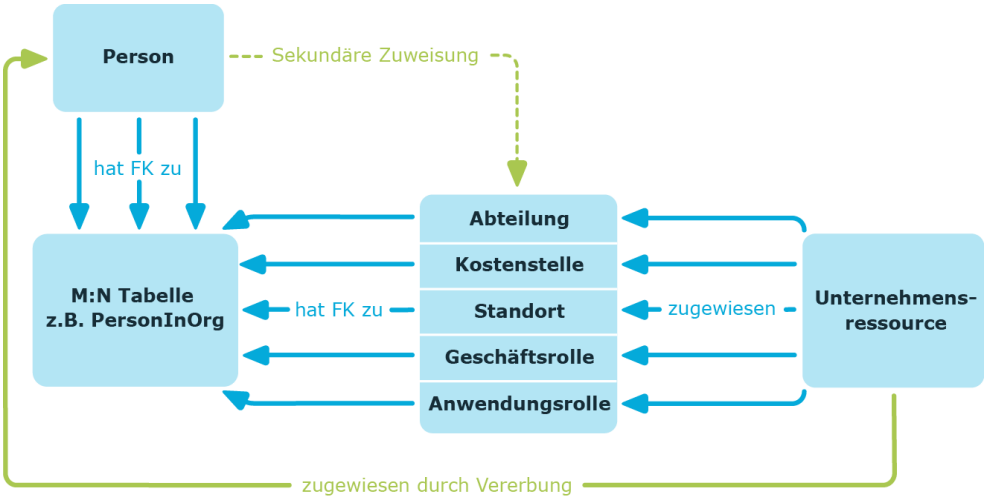
Verwandte Themen

- Sekundäre Zuweisung auf Seite 18
- Primäre Zuweisung auf Seite 18

Sekundäre Zuweisung

Die sekundäre Zuweisung erfolgt über die Einordnung einer Person, eines Gerätes oder eines Arbeitsplatzes in eine Rollenhierarchie. Die sekundäre Zuweisung ist das Standardverfahren für die Zuweisung und Vererbung von Unternehmensressourcen über Rollen. Ob eine sekundäre Zuweisung von Unternehmensressourcen an Personen, Geräte und Arbeitsplätze möglich ist, legen Sie an den Rollenklassen für Abteilungen, Standorte, Kostenstellen, Geschäftsrollen und Anwendungsrollen fest.

Abbildung 7: Schema einer sekundären Zuweisung



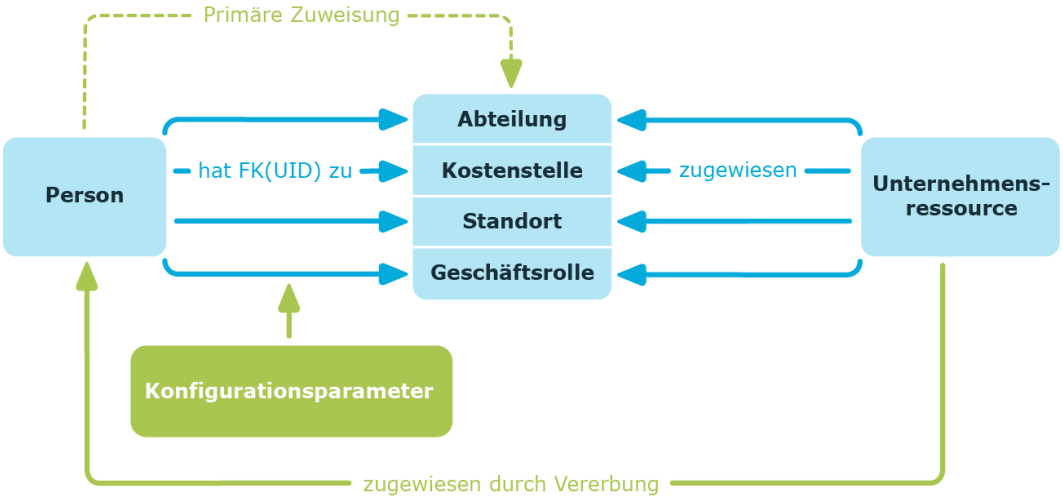
Verwandte Themen

- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Primäre Zuweisung

Die primäre Zuweisung erfolgt über die Fremdschlüssel-Referenzierung einer Abteilung, Kostenstelle oder eines Standortes in den Personen-, Geräte- und Arbeitsplatzobjekten. Dazu nutzen Sie die Eingabefelder für Rollen auf den Stammdatenformularen für Personen, Geräte und Arbeitsplätze. Die Vererbung über die primären Zuweisungen kann über Konfigurationsparameter aktiviert werden. Für Personenobjekte ist die primäre Zuweisung standardmäßig aktiv.

Abbildung 8: Schema einer primären Zuweisung



HINWEIS: Die Änderung der Konfigurationsparameter führt zu einer Neuberechnung der Vererbungsdaten! Das bedeutet: Wenn die primäre Zuweisung zu einem späteren Zeitpunkt wieder deaktiviert wird, werden die über diesen Weg entstandenen Vererbungsdaten aus der Datenbank entfernt.

Tabelle 1: Konfigurationsparameter für die primäre Zuweisung

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | Person	Personen können über primäre Zuweisung erben.
QER | Structures | Inherite | Person | FromDepartment	Personen erben die Zuordnungen von ihrer primären Abteilung (Person.UID_Department).
QER | Structures | Inherite | Person | FromLocality	Personen erben die Zuordnungen von ihrem primären Standort (Person.UID_Locality).
QER | Structures | Inherite | Person | FromProfitCenter	Personen erben die Zuordnungen von ihrer primären Kostenstelle (Person.UID_ProfitCenter).
QER | Structures | Inherite | Hardware	Geräte können über primäre Zuweisung erben.
QER | Structures | Inherite | Hardware | FromDepartment	Geräte erben die Zuordnungen von ihrer primären Abteilung (Hardware.UID_Department).
QER | Structures | Inherite | Hardware | FromLocality	Geräte erben die Zuordnungen von ihrem primären Standort (Hardware.UID_Locality).
QER | Structures | Inherite | Hardware | FromProfitCenter	Geräte erben die Zuordnungen von ihrer primären Kostenstelle (Hardware.UID_ProfitCenter).
QER | Structures | Inherite | Workdesk	Arbeitsplätze können über primäre Zuweisung erben.

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | Workdesk | FromDepartment	Arbeitsplätze erben die Zuordnungen von ihrer primären Abteilung (Workdesk.UID_Department).
QER | Structures | Inherite | Workdesk | FromLocality	Arbeitsplätze erben die Zuordnungen von ihrem primären Standort (Workdesk.UID_Locality).
QER | Structures | Inherite | Workdesk | FromProfitCenter	Arbeitsplätze erben die Zuordnungen von ihrer primären Kostenstelle (Workdesk.UID_ProfitCenter).

Zuweisung von Unternehmensressourcen über dynamische Rollen

Die Zuweisung über dynamische Rollen ist ein Spezialfall der indirekten Zuweisung. Dynamische Rollen werden eingesetzt, um Rollenmitgliedschaften dynamisch festzulegen. Dabei werden Personen, Geräte oder Arbeitsplätze nicht fest an eine Rolle zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen. Welche Personen, Geräte oder Arbeitsplätze diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Personen einer Abteilung zugewiesen werden; verlässt eine Person diese Abteilung, verliert sie sofort die zugewiesenen Unternehmensressourcen.

Verwandte Themen

- Dynamische Rollen auf Seite 37

Zuweisung von Unternehmensressourcen über IT Shop Bestellungen

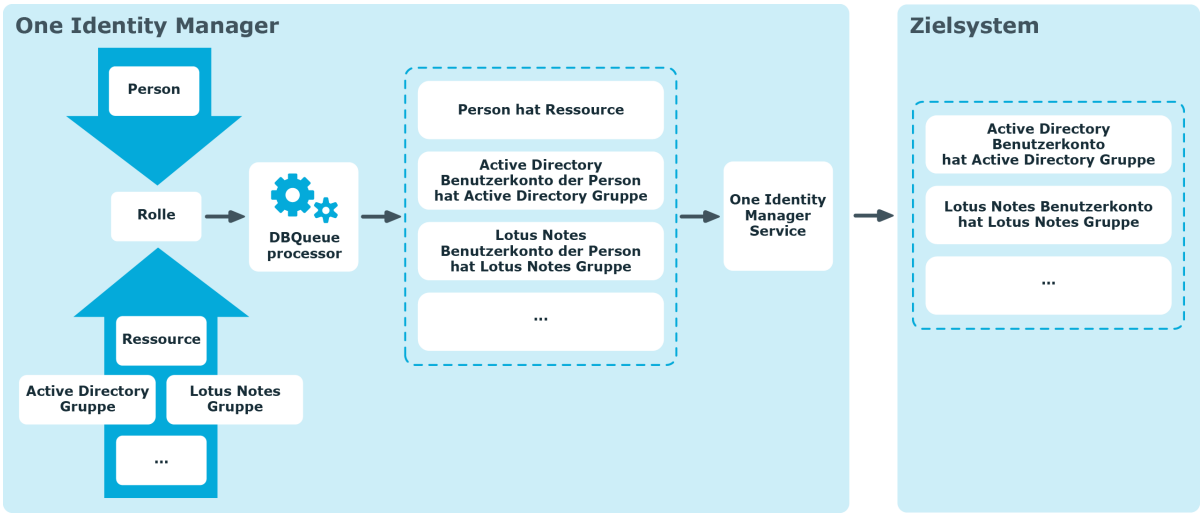
Die Zuweisung über IT Shop Bestellungen ist ein Spezialfall der indirekten Zuweisung. Damit Unternehmensressourcen über IT Shop Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Unternehmensressourcen, die als Produkte diesem Shop zugeordnet sind, können von den Kunden bestellt werden. Bestellte Unternehmensressourcen werden nach erfolgreicher Genehmigung den Personen zugewiesen. Neben den Unternehmensressourcen können über den IT Shop auch Rollenmitgliedschaften bestellt werden.

Abbildung 9: Schema einer Zuweisung über Bestellungen

Grundlagen zur Berechnung der Vererbung

Die Berechnung der durch die Vererbung zugeordneten Objekte erfolgt durch den DBQueue Prozessor. Durch Trigger werden bei vererbungsrelevanten Zuordnungen Aufträge in die DBQueue eingestellt. Diese Aufträge werden durch den DBQueue Prozessor verarbeitet und resultieren in weiteren Folgeaufträgen für die DBQueue oder in Prozessen für die Prozesskomponente `HandleObjectComponent` in der Jobqueue. Durch die Prozessverarbeitung werden die resultierenden Zuordnungen von Berechtigungen zu Benutzerkonten in den Zielsystem-Umgebungen eingefügt, geändert oder gelöscht.

Abbildung 10: Überblick über die Berechnung der Vererbung



Detaillierte Informationen zum Thema

- Berechnung der Vererbung über hierarchische Rollen auf Seite 22
- Berechnung der Zuweisungen auf Seite 23

Berechnung der Vererbung über hierarchische Rollen

Personen, Geräte und Arbeitsplätze können nur Mitglieder in Rollen werden, die auf der Tabelle BaseTree aufbauen. Diese Rollen werden in Sichten (Views) abgebildet, die jeweils einen bestimmten Teilausschnitt der Tabelle BaseTree repräsentieren. Zur Abbildung von Unternehmensstrukturen enthält das Datenmodell des One Identity Manager die folgenden Sichten:

Tabelle 2: Sichten auf die Tabelle BaseTree

Sicht	Bedeutung
Department	Abbildung von Abteilungen
Locality	Abbildung von Standorten
Profitcenter	Abbildung von Kostenstellen
Org	Abbildung von Geschäftsrollen
AERole	Abbildung von Anwendungsrollen

HINWEIS: Da die Sichten Teilausschnitte der Tabelle BaseTree sind, gelten alle nachfolgend beschriebenen Vererbungsmechanismen ebenso für die Sichten.

Vererbungen gehen von der Tabelle BaseTree aus. Die Tabelle BaseTree kann über die Beziehung UID_Org - UID_ParentOrg beliebig viele Rollenhierarchien abbilden. Diese werden in der Tabelle BaseTreeCollection abgelegt. Dabei werden alle Rollen aufgezählt, von denen die angegebene Rolle erbt. Entsprechend ihrer Teilausschnitte aus der Tabelle BaseTree gibt es für jede Sicht eine entsprechend benannte *Collection-Tabelle mit dem Teilausschnitt der Rollenhierarchie.

In der Tabelle BaseTreeCollection gilt folgende Beziehung:

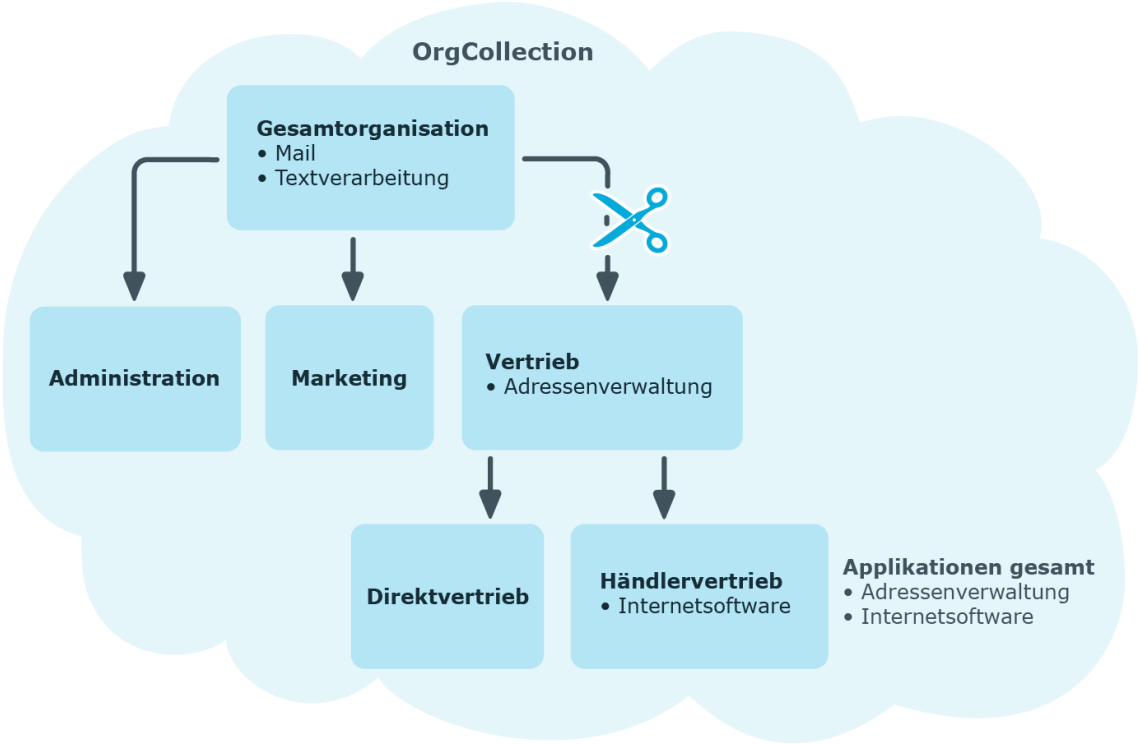
- UID_Org ist die Rolle, die erbt.
- UID_ParentOrg ist die Rolle, die vererbt.

Dieses Prinzip gilt auch bei Bottom-Up-Bäumen, die von unten nach oben vererben, auch wenn scheinbar die Eltern-Beziehung aus der BaseTree-Tabelle umgekehrt wird.

Jede Rolle erbt auch von sich selbst.

Jede Rolle einer Rollenhierarchie muss einen Bezug zur Tabelle OrgRoot (Rollenklassen) haben. OrgRoot ist die Klammer für Rollenhierarchien. Eine Rollenhierarchie wird immer nur für eine Rollenklasse gebildet. Rollen aus verschiedenen Rollenklassen dürfen nicht in ein und derselben Rollenhierarchie vorkommen oder per Eltern-Kind-Beziehung aufeinander verweisen.

Abbildung 11: Darstellung einer hierarchischen Rollenstruktur am Beispiel einer OrgCollection



Eine Rolle erbt alles, was ihren Eltern in der Rollenhierarchie zugewiesen wurde, einschließlich dem, was ihr selbst zugewiesen wurde. Ändert sich die Menge der Rollen, von denen eine Rolle etwas erbt, so wird für alle Mitglieder dieser Rolle eine Neuberechnung der zugeordneten Objekte veranlasst. Ändert sich die Menge von zugeordneten Objekten eines Objekttyps zu einer Rolle, so wird für alle Mitglieder der Rolle eine Neuberechnung der zugeordneten Objekte dieses Objekttyps veranlasst. Wird also beispielsweise Software an eine übergeordnete Rolle zugewiesen, werden die Mitglieder der Tabelle `BaseTreeHasApp` neu berechnet.

Die Mitglieder einer Rolle erben nach definierten Regeln alle Zuweisungen über die primären und sekundären Rollenstrukturen, denen Sie laut der Tabelle `BaseTree` angehören sowie den Vorgängerstrukturen laut der Tabelle `BaseTreeCollection`.

Berechnung der Zuweisungen

Bei der Berechnung der Vererbung erfolgt für jede Zuweisung ein Eintrag in die entsprechende Zuweisungstabelle. Jede Tabelle, in der Zuweisungen abgebildet werden, hat eine Spalte `XOrigin`. In dieser Spalte wird die Herkunft einer Zuweisung als Verknüpfung von Bit-Positionen abgelegt. Bei jedem Eintrag in die Zuweisungstabelle erfolgt entsprechend der Zuweisungsart eine Änderung der Bit-Positionen. Jede Zuweisungsart ändert dabei nur die für sie vorgesehene Bit-Position.

Es bedeuten:

- Bit 0: Die Zuweisung wurde direkt vorgenommen.
- Bit 1: Die Zuweisung wurde indirekt vorgenommen, jedoch nicht über eine dynamischen Rolle.
- Bit 2: Die Zuweisung erfolgte über eine dynamische Rolle.
- Bit 3: Die Zuweisung erfolgte über eine Zuweisungsbestellung.
- Bit 4: Das Bit wird modulspezifisch unterschiedlich verwendet. Ausführliche Informationen finden Sie in den Administrationshandbüchern der Module, in denen das Bit genutzt wird.

Tabelle 3: Mögliche Werte der Spalte XOrigin

Bit 3	Bit 2	Bit 1	Bit 0	Wert in XOrigin	Bedeutung
0	0	0	1	**1**	Nur direkt zugewiesen.
0	0	1	0	**2**	Nur indirekt zugewiesen.
0	0	1	1	**3**	Direkt und indirekt zugewiesen.
0	1	0	0	**4**	Über dynamische Rolle zugewiesen.
0	1	0	1	**5**	Über dynamische Rolle und direkt zugewiesen.
0	1	1	0	**6**	Über dynamische Rolle und indirekt zugewiesen.
0	1	1	1	**7**	Über dynamische Rolle, direkt und indirekt zugewiesen.
1	0	0	0	**8**	Zuweisungsbestellung.
1	0	0	1	**9**	Zuweisungsbestellung und direkt zugewiesen.
1	0	1	0	**10**	Zuweisungsbestellung und indirekt zugewiesen.
1	0	1	1	**11**	Zuweisungsbestellung, direkt und indirekt zugewiesen.
1	1	0	0	**12**	Zuweisungsbestellung und über dynamische Rolle zugewiesen.
1	1	0	1	**13**	Zuweisungsbestellung, direkt und über dynamische Rolle zugewiesen.
1	1	1	0	**14**	Zuweisungsbestellung, indirekt und über dynamische Rolle zugewiesen.
1	1	1	1	**15**	Zuweisungsbestellung, direkt, indirekt und über dynamische Rolle zugewiesen.

Besonderheiten bei Vererbung von Zuweisungen über Rollenhierarchie

HINWEIS: Wenn eine Zuweisung über die Rollenhierarchie vererbt wird, wird an der geerbten Zuweisung das **Bit 1** gesetzt. Geerbte Zuweisungen sind folglich immer indirekt zugewiesen, auch wenn sie ursprünglich direkt, über eine dynamische Rolle oder eine Zuweisungsbestellung entstanden sind.

Beispiel:

Für den Standort "Europe" wurde die Zuweisung einer Active Directory Gruppe bestellt. Der untergeordnete Standort "Madrid" erbt diese Zuweisung. In der Tabelle `LocalityHasADSGroup` ist `XOrigin` folgendermaßen gesetzt:

- Standort "Europe": `XOrigin='8'` (Zuweisungsbestellung)
- Standort "Madrid": `XOrigin='2'` (indirekt zugewiesen)

Wirksamkeit von Zuweisungen

Ob eine Zuweisung wirksam ist, wird über die Spalte `XIsInEffect` abgebildet. Ist beispielsweise eine Person deaktiviert, zum Löschen markiert oder als sicherheitsgefährdend eingestuft, so kann für diese Person die Vererbung der Unternehmensressourcen unterbunden werden. Die Zuweisung der Gruppen bleibt erhalten, diese Zuweisung wird jedoch nicht wirksam.

Der DBQueue Prozessor überwacht die Änderung der Spalte `XOrigin`. Bei Änderung des Wertes in `XOrigin` wird die Spalte `XIsInEffect` neu berechnet.

Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen

Der One Identity Manager liefert eine Konfiguration, die den sofortigen Einsatz von hierarchischen Rollen für Abteilungen, Kostenstellen, Standorte und Anwendungsrollen unterstützt. Abhängig von der Unternehmensstruktur, kann es jedoch erforderlich sein, zusätzliche Festlegungen für die Zuweisungen zu Rollen treffen.

Folgende Einstellungen sollten Sie vor der Zuweisung von Unternehmensressourcen prüfen und gegebenenfalls anpassen:

- Legen Sie fest, ob und wie Personen, Geräte und Arbeitsplätze und Unternehmensressourcen an Rollen zugewiesen werden dürfen.

  Für Abteilungen, Kostenstellen, Standorte und Anwendungsrollen sind Zuweisungen von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen vordefiniert.

Die Konfiguration für Zuweisungen zu Anwendungsrollen kann nicht geändert werden.

- Legen Sie die Vererbungsrichtung innerhalb der Hierarchie fest.

  Für Abteilungen, Kostenstellen, Standorte und Anwendungsrollen ist eine Top-Down Vererbung definiert.

- Schränken Sie bei Bedarf die Vererbung für bestimmte Rollen ein.

  Sie können für einzelne Rollen oder einzelne Personen, Geräte oder Arbeitsplätze festlegen, ob die Vererbung von Unternehmensressourcen verhindert werden soll.

- Definieren Sie bei Bedarf Rollen, die sich gegenseitig ausschließen.

  Über die Festlegung sogenannter widersprechende Rollen verhindern Sie, dass Personen, Geräte oder Arbeitsplätze in Rollen aufgenommen werden, die sich ausschließende Unternehmensressourcen enthalten.

Detaillierte Informationen zum Thema

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 26
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31
- Vererbung über Rollen blockieren auf Seite 32
- Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern auf Seite 33
- Vererbung an einzelne Personen, Geräte oder Arbeitsplätze verhindern auf Seite 34
- Vererbungsausschluss: Festlegen widersprechender Rollen auf Seite 35

Mögliche Zuweisungen von Unternehmensressourcen über Rollen

Personen, Geräte und Arbeitsplätze können über indirekte Zuweisung Unternehmensressourcen erhalten. Dazu sind Personen, Geräte und Arbeitsplätze in beliebig viele Rollen eingeordnet. Über definierte Regeln erhalten die Personen, Geräte und Arbeitsplätze die entsprechenden Unternehmensressourcen.

Um Unternehmensressourcen an Rollen zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Rollen.

In der nachfolgenden Tabelle sind die möglichen Zuweisungen von Unternehmensressourcen an Personen, Geräte und Arbeitsplätze über Rollen dargestellt.

> HINWEIS: Die Unternehmensressourcen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 4: Mögliche Zuweisungen von Unternehmensressourcen über Rollen

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	**Arbeitsplätze**
Ressourcen	möglich	-
Kontendefinitionen	möglich	
Gruppen kundendefinierter Zielsysteme	möglich (Zuweisung an alle Benutzerkonten kundendefinierter Zielsysteme einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
Systemberechtigungen kundendefinierter Zielsysteme	möglich (Zuweisung an alle Benutzerkonten kundendefinierter Zielsysteme einer Person, für welche die Vererbung von Systemberechtigungen zugelassen ist)	-
Active Directory Gruppen	möglich (Zuweisung an alle Active Directory Benutzerkonten und Active Directory Kontakte einer Person, für welche die Vererbung von Active Directory Gruppen zugelassen ist)	-
SharePoint Gruppen	möglich (Zuweisung an alle SharePoint Benutzerkonten einer Person, für welche die Vererbung von SharePoint Gruppen zugelassen ist)	-
SharePoint Rollen	möglich (Zuweisung an alle SharePoint Benutzerkonten einer Person, für welche die Vererbung von SharePoint Rollen zugelassen ist)	-
LDAP Gruppen	möglich (Zuweisung an alle LDAP Benutzerkonten einer Person, für welche die Vererbung von LDAP Gruppen zugelassen ist)	-
Notes Gruppen	möglich (Zuweisung an alle Notes Benutzerkonten einer Person, für welche die Vererbung von Notes Gruppen zugelassen ist)	-
SAP Gruppen	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen und für	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	Arbeitsplätze
	welche die Vererbung von SAP Gruppen zugelassen ist)	
SAP Profile	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen und für welche die Vererbung von SAP Profilen zugelassen ist)	-
SAP Rollen	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen und für welche die Vererbung von SAP Rollen zugelassen ist)	-
SAP Parameter	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP System liegen)	-
Strukturelle Profile	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen und für welche die Vererbung von strukturellen Profilen zugelassen ist)	-
BI Analyseberechtigungen	möglich (Zuweisung an alle BI Benutzerkonten einer Person, die im selben System liegen und für welche die Vererbung von Gruppen zugelassen ist)	-
Azure Active Directory Gruppen	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Azure Active Directory Gruppen zugelassen ist)	-
Azure Active Directory Administratorrollen	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Azure Active Directory Administratorrollen zugelassen ist)	-
Azure Active Directory Abonnements	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	Arbeitsplätze
	Vererbung von Azure Active Directory Abonnements zugelassen ist)	
Unwirksame Azure Active Directory Dienstpläne	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von unwirksamen Azure Active Directory Dienstplänen zugelassen ist)	-
Cloud Gruppen	möglich (Zuweisung an alle Cloud Benutzerkonten einer Person, für welche die Vererbung von Cloud Gruppen zugelassen ist)	-
Cloud Systemberechtigungen	möglich (Zuweisung an alle Cloud Benutzerkonten einer Person, für welche die Vererbung von Cloud Systemberechtigungen zugelassen ist)	-
Unix Gruppen	möglich (Zuweisung an alle Unix Benutzerkonten einer Person, für welche die Vererbung von Unix Gruppen zugelassen ist)	-
E-Business Suite Berechtigungen	möglich (Zuweisung an alle E-Business Suite Benutzerkonten einer Person, die im selben E-Business Suite System liegen und für welche die Vererbung von E-Business Suite Gruppen zugelassen ist)	-
PAM Benutzergruppen	möglich (Zuweisung an alle PAM Benutzerkonten einer Person, für welche die Vererbung von PAM Gruppen zugelassen ist)	-
Google Workspace Produkte und SKUs	möglich (Zuweisung an alle Google Workspace Benutzerkonten einer Person, die in der selben Kunden-Umgebung liegen und für welche die Vererbung von Google Workspace Produkten und SKUs zugelassen ist)	-
Google Workspace Gruppen	möglich (Zuweisung an alle Google	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	Arbeitsplätze
	Workspace Benutzerkonten einer Person, die in der selben Kunden-Umgebung liegen und für welche die Vererbung von Google Workspace Gruppen zugelassen ist)	
SharePoint Online Gruppen	möglich (Zuweisung an alle SharePoint Online Benutzerkonten einer Person, für welche die Vererbung von SharePoint Online Gruppen zugelassen ist)	-
SharePoint Online Rollen	möglich (Zuweisung an alle SharePoint Online Benutzerkonten einer Person, für welche die Vererbung von SharePoint Online Rollen zugelassen ist)	-
Office 365 Gruppen	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Office 365 Gruppen zugelassen ist)	-
Exchange Online E-Mail aktivierte Verteilergruppen	möglich (Zuweisung an alle an Exchange Online Postfächer, Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte einer Person, für welche die Vererbung von Exchange Online E-Mail aktivierten Verteilergruppen zugelassen ist)	-
Systemrollen	möglich	möglich
Abonnierbare Berichte	möglich	-
Software	möglich	möglich

Verwandte Themen

- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88

Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben

Das Standardverfahren für die Zuweisung von Unternehmensressourcen über Rollen ist die sekundäre Zuweisung. Dafür werden sowohl Personen, Geräte und Arbeitsplätze als auch die Unternehmensressourcen über die sekundäre Zuweisung in die Rollen aufgenommen.

Ob und wie Personen, Geräte, Arbeitsplätze und Unternehmensressourcen an Rollen sekundär zugewiesen werden dürfen, legen Sie über die Rollenklasse fest. Rollenklassen bilden die Basis für die Abbildung von hierarchischen Rollen im One Identity Manager. Rollenklassen dienen zur Zusammenfassung gleichartiger Rollen. Folgende Rollenklassen sind standardmäßig im One Identity Manager vorhanden:

- Abteilung
- Kostenstelle
- Standort
- Anwendungsrolle

Die sekundäre Zuweisung von Objekten zu Rollen einer Rollenklasse wird über folgende Optionen definiert:

- **Zuweisungen erlaubt:** Mit dieser Option legen Sie fest, ob die Zuweisung der jeweiligen Objekttypen zu Rollen der Rollenklasse generell erlaubt ist.
- **Direkte Zuweisungen erlaubt**: Mit dieser Option legen Sie fest, ob die jeweiligen Objekttypen direkt an die Rollen der Rollenklasse zugewiesen werden können. Sollen beispielsweise Ressourcen über die Zuweisungsformulare im Manager an Abteilungen, Kostenstellen oder Standorte zugewiesen werden, dann setzen Sie diese Option.

  HINWEIS: Ist die Option nicht gesetzt, dann ist die Zuweisung des jeweiligen Objekttyps nur über Bestellungen im IT Shop, dynamische Rollen oder Systemrollen möglich.

Beispiel:

Um Personen im Manager direkt an Abteilungen zuzuweisen, aktivieren Sie an der Rollenklasse **Abteilung**, für den Eintrag **Personen** die Optionen **Zuweisungen erlaubt** und **Direkte Zuweisungen erlaubt**.

Sollen Personen die Mitgliedschaft in einer Abteilung nur über den IT Shop erhalten, dann aktivieren Sie an der Rollenklasse **Abteilung**, für den Eintrag **Personen**, die Option **Zuweisungen erlaubt** und deaktivieren die Option **Direkte Zuweisungen**

erlaubt. Im IT Shop muss dann eine entsprechende Zuweisungsressource verfügbar sein.

HINWEIS: Für Abteilungen, Kostenstellen, Standorte und Anwendungsrollen sind Zuweisungen von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen vordefiniert. Die Konfiguration für Zuweisungen zu Anwendungsrollen kann nicht geändert werden.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren**.
3. Verwenden Sie die Spalte **Zuweisungen erlaubt** um festzulegen, ob eine Zuweisung generell erlaubt ist.

   HINWEIS: Sie können die Option **Zuweisungen erlaubt** nur dann deaktivieren, wenn es keine Zuweisungen der jeweiligen Objekte zu Rollen dieser Rollenklasse gibt oder über bestehende dynamische Rollen entstehen könnten.
4. Verwenden Sie die Spalte **Direkte Zuweisungen erlaubt** um festzulegen, ob eine direkte Zuweisung erlaubt ist.

   HINWEIS: Sie können die Option **Direkte Zuweisungen erlaubt** nur dann deaktivieren, wenn es keine direkten Zuweisungen der jeweiligen Objekte zu Rollen der Rollenklasse gibt.
5. Speichern Sie die Änderungen.

Vererbung über Rollen blockieren

In speziellen Fällen ist die Vererbung über mehrere Hierarchieebenen nicht gewünscht. Deshalb ist die Unterbrechung der Vererbung innerhalb einer Hierarchie möglich. Abhängig von der Vererbungsrichtung hat diese Festlegung unterschiedliche Auswirkungen.

- Bei einer Top-Down-Vererbung erbt die mit der Option **Vererbung blockieren** versehene Rolle keine Zuweisungen aus der übergeordneten Ebene. Sie vererbt die ihr direkt zugewiesenen Unternehmensressourcen ihrerseits jedoch an die ihr untergeordneten Ebenen weiter.
- In einer Bottom-Up-Vererbung erbt die mit der Option **Vererbung blockieren** versehene Rolle alle Zuweisungen der untergeordneten Ebenen. Die Rolle selbst vererbt jedoch keinerlei Zuweisungen weiter nach oben.

Um die Vererbung für Abteilungen, Kostenstellen oder Standorte zu unterbrechen

1. Wählen Sie im Manager in der Kategorie **Organisationen** die Abteilung, die Kostenstelle oder den Standort.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Aktivieren Sie die Option **Vererbung blockieren**.
4. Speichern Sie die Änderungen.

HINWEIS: Für Anwendungsrollen kann die Vererbung nur für kundenspezifische Anwendungsrollen unterbrochen werden. Ausführliche Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Verwandte Themen

- Unterbrechen der Vererbung auf Seite 14
- Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern auf Seite 33
- Vererbung an einzelne Personen, Geräte oder Arbeitsplätze verhindern auf Seite 34

Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern

Für einzelne Rollen kann die Vererbung von Unternehmensressourcen vorübergehend verhindert werden. Dieses Verhalten können Sie beispielsweise nutzen, um alle erforderlichen Unternehmensressourcen an eine Rolle zuzuweisen. Die Vererbung der Unternehmensressourcen erfolgt jedoch erst dann, wenn die Vererbung für diese Rolle wieder zugelassen wird, beispielsweise nach Durchlaufen eines definierten Freigabeprozesses.

Um die Vererbung für Abteilungen, Kostenstellen oder Standorte zu verhindern

1. Wählen Sie im Manager in der Kategorie **Organisationen** die Abteilung, die Kostenstelle oder den Standort.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Aktivieren Sie eine oder mehrere der folgenden Optionen.
    - Um die Vererbung an Personen zu verhindern, aktivieren Sie die Option **Keine Vererbung an Personen**.
    - Um die Vererbung an Geräte zu verhindern, aktivieren Sie die Option **Keine Vererbung an Geräte**.
    - Um die Vererbung an Arbeitsplätze zu verhindern, aktivieren Sie die Option **Keine Vererbung an Arbeitsplätze**.
4. Speichern Sie die Änderungen.

HINWEIS: Für Anwendungsrollen können diese Optionen nicht konfiguriert werden. Ausführliche Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Verwandte Themen

- Vererbung über Rollen blockieren auf Seite 32
- Vererbung an einzelne Personen, Geräte oder Arbeitsplätze verhindern auf Seite 34

Vererbung an einzelne Personen, Geräte oder Arbeitsplätze verhindern

Für einzelne Personen, Geräte oder Arbeitsplätze kann die Vererbung von Unternehmensressourcen verhindert werden. Dieses Verhalten können Sie beispielsweise nutzen, um nach einem Personenimport die importierten Daten zunächst zu korrigieren und erst anschließend die Vererbung freizuschalten.

Um die Vererbung für eine Person zu verhindern

1. Wählen Sie im Manager in der Kategorie **Personen** die Person.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Aktivieren Sie die Option **Keine Vererbung**.

   Die Person erbt keine Unternehmensressourcen über Rollen.

   HINWEIS: Diese Option hat keinen Einfluss auf direkte Zuweisungen! Direkt zugewiesene Unternehmensressourcen bleiben zugewiesen.
4. Speichern Sie die Änderungen.

Um die Vererbung für ein Gerät zu verhindern

1. Wählen Sie im Manager in der Kategorie **Geräte & Arbeitsplätze > Geräte** das Gerät.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Aktivieren Sie die Option **Keine Vererbung**.

   Das Gerät erbt keine Unternehmensressourcen über Rollen.

   HINWEIS: Diese Option hat keinen Einfluss auf direkte Zuweisungen! Direkt zugewiesene Unternehmensressourcen bleiben zugewiesen.
4. Speichern Sie die Änderungen.

Um die Vererbung für einen Arbeitsplatz zu verhindern

1. Wählen Sie im Manager in der Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze** den Arbeitsplatz.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

3. Aktivieren Sie die Option **Keine Vererbung**.

   Der Arbeitsplatz erbt keine Unternehmensressourcen über Rollen.

   HINWEIS: Diese Option hat keinen Einfluss auf direkte Zuweisungen! Direkt zugewiesene Unternehmensressourcen bleiben zugewiesen.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Vererbung über Rollen blockieren auf Seite 32
- Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern auf Seite 33

Vererbungsausschluss: Festlegen widersprechender Rollen

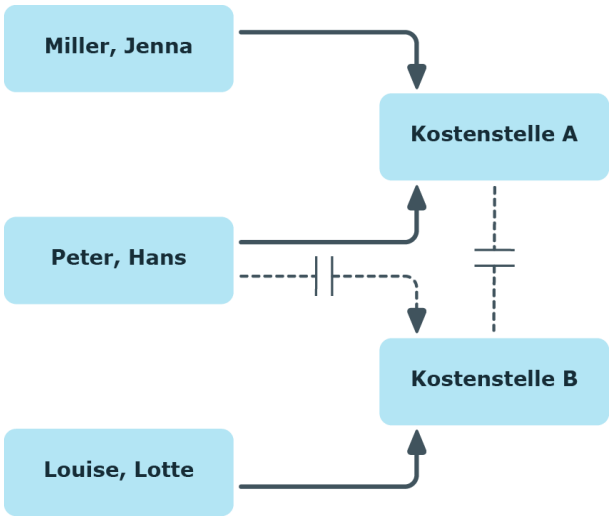
Um zu verhindern, dass Personen, Geräte oder Arbeitsplätze gleichzeitig an verschiedene Rollen zugewiesen werden und über diese Rollen sich ausschließende Unternehmensressourcen erhalten könnten, können Sie widersprechende Rollen definieren. Dabei legen Sie fest, welche Abteilungen, Kostenstellen oder Standorte sich gegenseitig ausschließen. Sie dürfen diese Rollen dann nicht mehr an ein und dieselbe Person (Gerät, Arbeitsplatz) zuweisen.

HINWEIS: Nur Rollen, die direkt als widersprechende Rollen definiert sind, können nicht an ein und dieselbe Person (Gerät, Arbeitsplatz) zugewiesen werden. Festlegungen an übergeordneten oder untergeordneten Rollen haben keinen Einfluss auf die Zuweisung.

Beispiel:

An der Kostenstelle A wurde Kostenstelle B als widersprechende Kostenstelle eingetragen. Jenna Miller und Hans Peter sind Mitglied der Kostenstelle A. Lotte Louise ist Mitglied der Kostenstelle B. Hans Peter kann nicht an Kostenstelle B zugewiesen werden. Der One Identity Manager verhindert außerdem, dass Jenna Miller an Kostenstelle B und Lotte Louise an Kostenstelle A zugewiesen wird.

Abbildung 12: Mitgliedschaften in sich widersprechenden Rollen



Um den Vererbungsausschluss zu konfigurieren

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Structures | ExcludeStructures** und kompilieren Sie die Datenbank.

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

Verwandte Themen

- Vererbungsausschluss für Abteilungen, Kostenstellen und Standorte festlegen auf Seite 94

Dynamische Rollen

Dynamische Rollen werden eingesetzt, um Mitgliedschaften für Abteilungen, Kostenstellen, Standort, Geschäftsrollen, Anwendungsrollen und IT Shop Knoten dynamisch festzulegen. Dabei werden Personen, Geräte oder Arbeitsplätze nicht fest an diese Rollen zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen. Welche Personen (Geräte oder Arbeitsplätze) diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Personen einer Abteilung zugewiesen werden; verlässt eine Person diese Abteilung verliert sie sofort die zugewiesenen Unternehmensressourcen.

Beispiel: Funktion dynamischer Rollen

In einer neu angelegten dynamischen Rolle werden alle externen Personen zusammengefasst. Diesen Personen soll eine Unternehmensressource ABC zugewiesen werden. Zunächst wird die dynamische Rolle mit folgenden Angaben definiert:

Dynamische Rolle	Externe Personen
Beschreibung	Alle externen Personen
Objektklasse	PERSON
Bedingung	IsExternal = 1
Abteilung	A_1

Der Abteilung A_1 wird nun die Ressource ABC zugewiesen. Alle Personen, die zum Zeitpunkt der Definition der dynamischen Rolle die Bedingung erfüllen, werden der Abteilung A_1 zugeordnet und erben von ihr die Ressource ABC. Erfüllen zu einem späteren Zeitpunkt weitere Personen die Bedingung, so werden diese Personen ab dem Moment in die Abteilung A_1 aufgenommen. Umgekehrt gilt jedoch auch, dass Personen aus der Abteilung A_1 entfernt werden, sobald sie im One Identity Manager nicht mehr als externe Personen bekannt sind. Sofern den Personen die Ressource

ABC nicht noch über einen anderen Weg zugewiesen wurde, ist die Ressource ab diesem Zeitpunkt nicht mehr verfügbar.

Rollenmitgliedschaften über dynamische Rollen werden als indirekte, sekundäre Zuweisung realisiert. Daher muss die sekundäre Zuweisung von Personen, Geräten und Arbeitsplätzen an den Rollenklassen zugelassen sein. Gegebenenfalls müssen Sie dazu weitere Konfigurationseinstellungen vornehmen.

Personen können aufgrund einer abgelehnten Attestierung oder einer Regelverletzung automatisch aus dynamischen Rollen ausgeschlossen werden. Dafür wird eine Ausschlussliste geführt. Zusätzlich können Ausschlüsse auch direkt für einzelne Personen definiert werden. Personen können zusätzlich auch direkt oder durch eine Zuweisungsbestellung oder Delegierung Mitglied der Rolle werden. Diese Mitgliedschaften werden durch die Ausschlussliste nicht eingeschränkt.

Ausführliche Informationen zum automatischen Ausschluss bei abgelehnter Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*. Ausführliche Informationen zum automatischen Ausschluss bei einer Regelverletzung finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

Detaillierte Informationen zum Thema

- Dynamische Rollen erstellen und bearbeiten auf Seite 38
- Hinweise zu Bedingungen für dynamische Rollen auf Seite 39
- Bedingungen für dynamische Rollen testen auf Seite 41
- Berechnung der Rollenmitgliedschaften für dynamische Rollen auf Seite 41
- Personen aus dynamischen Rollen ausschließen auf Seite 51
- Überblick über dynamische Rollen anzeigen auf Seite 53
- Stammdaten für dynamische Rollen auf Seite 53

Verwandte Themen

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Dynamische Rollen erstellen und bearbeiten

Dynamische Rollen können Sie für Abteilungen, Kostenstellen, Standort, Geschäftsrollen, Anwendungsrollen und IT Shop Knoten erstellen. Damit können Sie Mitgliedschaften in diesen Rollen dynamisch festlegen.

Um eine dynamische Rolle zu erstellen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt werden soll.
2. Wählen Sie die Aufgabe **Dynamische Rolle erstellen**.
3. Erfassen Sie die erforderlichen Stammdaten.
4. Speichern Sie die Änderungen.

Um eine dynamische Rolle zu bearbeiten

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für diese Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Bearbeiten Sie die Daten und speichern Sie anschließend die Änderungen.

Verwandte Themen

- Hinweise zu Bedingungen für dynamische Rollen auf Seite 39
- Bedingungen für dynamische Rollen testen auf Seite 41
- Stammdaten für dynamische Rollen auf Seite 53
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten auf Seite 91

Hinweise zu Bedingungen für dynamische Rollen

WICHTIG: Umfasst die Bedingung eine große Anzahl zuzuordnender Objekte, kann bei der Berechnung der Mitgliedschaften eine hohe Last im DBQueue Prozessor und damit auf dem Datenbankserver erzeugt werden.

Die Bedingung einer dynamischen Rolle wird als gültige Where–Klausel für Datenbankabfragen definiert und muss sich auf die gewählte Objektklasse **Person**, **Hardware** oder **Worksdesk** beziehen.

Sie haben im Manager verschiedene Möglichkeiten die Bedingungen zu erstellen:

- Die Bedingung können Sie direkt als SQL-Abfrage eingeben.
- Sie können zum Erstellen der Bedingungen den Where-Klausel Assistenten nutzen.
- Bedingungen für Personenobjekte können Sie alternativ über den Filterdesigner zusammenstellen.

HINWEIS: Wenn Sie im Filterdesigner den Bedingungstyp **Für das Konto mit dem Zielsystemtyp** oder **Für die Berechtigung mit dem Zielsystemtyp** wählen, können nur Spalten ausgewählt werden, die im Unified Namespace abgebildet sind und für die die Spalteneigenschaft **Anzeige im Filterdesigner** aktiviert ist.

Über die Variable `@UID_Org` können Sie auf die Rolle oder die Organisation zugreifen, auf welche die dynamische Rolle verweist.

Beispiel:

Die Bedingung für die dynamische Rolle für Personen soll nur wirken, wenn der Standort der Person (`Person.UID_Locality`) und der Standort der zugeordnete Rolle oder Organisation (`BaseTree.UID.UID_OrgLocality`) übereinstimmen.

Ergänzung der Where-Klausel:

```
...
and uid_locality = (select b.UID_OrgLocality from BaseTree b where b.UID_Org
= @UID_Org)
```

Beispiel:

Die Bedingung für die dynamische Rolle für Personen soll nur wirken, solange die zugeordnete Rolle oder Organisation eine bestimmte Eigenschaft hat.

Ergänzung der Where-Klausel:

```
...
and exists (select top 1 1
from BaseTree b
where b.UID_Org = @UID_Org
and b.CustomProperty01 = '123'
)
```

HINWEIS: Wenn Sie Kommentare in die Bedingung einfügen und die Kommentarzeichen `--`, `//` oder `%` verwenden, kann der DBQueue Prozessor die dynamische Rolle nicht korrekt berechnen. Die Berechnung wird mit einem Fehler abgebrochen. Schließen Sie Kommentare immer mit den Kommentarzeichen `/* ... */` ein.

Verwandte Themen

- Bedingungen für dynamische Rollen testen auf Seite 41

Bedingungen für dynamische Rollen testen

HINWEIS: Um die Aufgabe auszuführen, benötigen die Benutzer die Programmfunktion **Common_AllowRiskyWhereClauses**.

HINWEIS: Diese Aufgabe ist nur sichtbar, wenn die Bedingung für die dynamische Rolle direkt als SQL-Abfrage angezeigt wird.

Vor dem Speichern einer dynamischen Rolle sollten Sie überprüfen, welche Objekte die angegebene Bedingung erfüllen.

Um die SQL-Bedingung für eine dynamische Rolle zu testen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Klicken Sie auf dem Stammdatenformular (**SQL bearbeiten**).

   Die Bedingung wird als SQL-Abfrage angezeigt.
6. Wählen Sie die Aufgabe **Bedingung testen**.

   Auf dem Stammdatenformular werden im Feld **Testergebnis** alle Objekte angezeigt, die durch die Bedingung ermittelt werden.

Verwandte Themen

- Hinweise zu Bedingungen für dynamische Rollen auf Seite 39

Berechnung der Rollenmitgliedschaften für dynamische Rollen

Um die Rollenmitgliedschaften zu berechnen, prüft der One Identity Manager zu jeder dynamischen Rolle, ob

- es mindestens ein Objekt gibt, das der Bedingung genügt, aber nicht der Rolle zugeordnet ist
- es mindestens ein Objekt gibt, das der Bedingung nicht genügt, aber der Rolle zugeordnet ist
- die Ausschlussliste geändert wurde

Ist eine der Bedingungen erfüllt, wird ein Auftrag zum Hinzufügen oder zum Löschen von Mitgliedschaften für den DBQueue Prozessor eingestellt.

HINWEIS: Bei der Prüfung der dynamischen Rollen werden Personenobjekte, die zum Löschen markiert sind:

- nicht über dynamische Rollen in Rollen aufgenommen, auch wenn die sonstige Bedingung erfüllt sein sollte
- aus der Rolle entfernt, auch wenn die sonstige Bedingung erfüllt sein sollte

Die Berechnung der Rollenmitgliedschaften in dynamischen Rollen kann über verschiedene Verfahren ausgelöst werden.

- Zyklische Überprüfung über einen Zeitplan
- Neuberechnung bei Änderung von Objekten
- Manueller Start der Neuberechnung

Verwandte Themen

- Zeitpläne zur Berechnung von dynamischen Rollen auf Seite 42
- Dynamische Rollen bei Änderungen von Objekten sofort berechnen auf Seite 47
- Rollenmitgliedschaften für dynamische Rollen sofort berechnen auf Seite 50
- Dynamische Rollen von der Neuberechnung ausschließen auf Seite 51
- Personen aus dynamischen Rollen ausschließen auf Seite 51

Zeitpläne zur Berechnung von dynamischen Rollen

HINWEIS: Wenn ein Zeitplan gestartet wird, werden Neuberechnungen für alle dynamischen Rollen ausgeführt, denen der Zeitplan zugeordnet ist und für die die Option **Keine Neuberechnung von Zuweisungen** nicht aktiviert ist.

In der Standardinstallation des One Identity Manager ist bereits der Zeitplan **Berechnung dynamischer Rollen** definiert. Dieser Zeitplan wird beim Erstellen einer neuen dynamischen Rolle verwendet. Durch den Zeitplan werden die Rollenmitgliedschaften für alle dynamischen Rollen geprüft und nötigenfalls Aufträge zur Neuberechnung für den DBQueue Prozessor eingestellt. Die Überprüfung erfolgt in definierten Zeitabständen. Bei Bedarf können Sie den Standardzeitplan für dynamische Rollen ändern oder neue Zeitpläne erstellen.

Ausführliche Informationen zu Zeitplänen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Verwandte Themen

- Zeitpläne für dynamische Rollen erstellen und bearbeiten auf Seite 43
- Zeitpläne für dynamische Rollen sofort ausführen auf Seite 46
- Dynamische Rollen an Zeitpläne zuweisen auf Seite 47
- Dynamische Rollen bei Änderungen von Objekten sofort berechnen auf Seite 47
- Eigenschaften für die sofortige Neuberechnung bearbeiten auf Seite 49
- Rollenmitgliedschaften für dynamische Rollen sofort berechnen auf Seite 50
- Stammdaten für dynamische Rollen auf Seite 53

Zeitpläne für dynamische Rollen erstellen und bearbeiten

Bei Bedarf können Sie den Standardzeitplan für dynamische Rollen ändern oder neue Zeitpläne erstellen.

Um einen Zeitplan zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Zeitpläne**.

   In der Ergebnisliste werden alle Zeitpläne angezeigt, die für dynamische Rollen konfiguriert sind.
2. Wählen Sie in der Ergebnisliste einen Zeitplan und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Zeitplans.
4. Speichern Sie die Änderungen.

Um einen Zeitplan zu erstellen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Zeitpläne**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Zeitplans.
4. Speichern Sie die Änderungen.

Für einen Zeitplan bearbeiten Sie folgende Eigenschaften.

Tabelle 5: Eigenschaften für einen Zeitplan

Eigenschaft	Bedeutung
Bezeichnung	Bezeichnung des Zeitplanes.

Eigenschaft	Bedeutung
Beschreibung	Nähere Beschreibung des Zeitplans.
Aktiviert	Gibt an, ob der Zeitplan aktiv ist.
Zeitzone	Eindeutige Kennung der Zeitzone, nach dessen Zeitangaben der Zeitplan ausgeführt werden soll. Wählen Sie in der Auswahlliste zwischen **Universal Time Code** oder einer der Zeitzonen.
Beginn (Datum)	Tag, an dem der Zeitplan erstmalig ausgeführt werden soll. Falls sich dieser Tag mit dem definierten Intervalltyp widerspricht, ist die erstmalige Ausführung der nächste erreichbare Tag basierend auf dem Startdatum.
Gültigkeitszeitraum	Zeitraum, innerhalb dessen der Zeitplan ausgeführt werden soll. • Wenn der Zeitplan unbefristet ausgeführt werden soll, wählen Sie die Option **Unbegrenzte Laufzeit**. • Um einen Gültigkeitszeitraum festzulegen, wählen Sie die Option **Begrenzte Laufzeit** und erfassen Sie im Eingabefeld **Ende (Datum)** den Tag, an dem der Zeitplan letztmalig ausgeführt werden soll.

Auftreten	Intervall, in welchem der Auftrag ausgeführt wird. Abhängig vom gewählten Intervall sind weitere Einstellungen erforderlich.
	• **stündlich**: Der Zeitplan soll in einem definierten Intervall von Stunden ausgeführt werden, beispielsweise alle zwei Stunden.
	  • Legen Sie unter **Wiederholen alle** fest, nach wie vielen Stunden der Zeitplan wiederholt ausgeführt werden soll.
	  • Der Startzeitpunkt wird aus der Ausführungsfrequenz und dem Intervalltyp berechnet.
	• **täglich**: Der Zeitplan soll zu definierten Uhrzeiten in einem definierten Intervall von Tagen ausgeführt werden, beispielsweise jeden zweiten Tag um 6:00 Uhr und um 18:00 Uhr.
	  • Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll.
	  • Legen Sie unter **Wiederholen alle** fest, nach wie vielen Tagen der Zeitplan wiederholt werden soll.
	• **wöchentlich**: Der Zeitplan soll in einem definierten Intervall von Wochen, an einem bestimmten Wochentag, zu definierten Uhrzeiten ausgeführt werden, beispielsweise jede zweite Woche am Montag um 6:00 Uhr und um 18:00 Uhr.

Eigenschaft	Bedeutung
	• Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll. • Legen Sie unter **Wiederholen alle** fest, nach wie vielen Wochen der Zeitplan wiederholt ausgeführt werden soll. • Legen Sie den genauen Wochentag fest, an dem der Zeitplan ausgeführt werden soll. • **monatlich**: Der Zeitplan soll in einem definierten Intervall von Monaten, an bestimmten Tagen, zu definierten Uhrzeiten ausgeführt werden, beispielsweise jeden zweiten Monat am 1.Tag und am 15. Tag jeweils um 6:00 Uhr und um 18:00 Uhr. • Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll. • Legen Sie unter **Wiederholen alle** fest, nach wie vielen Monaten der Zeitplan wiederholt werden soll. • Legen Sie die Tage des Monats fest (1.-31. Tag eines Monats). HINWEIS: Wenn es beim Intervalltyp **monatlich** mit dem Subintervall **29**, **30** oder **31** den Ausführungstag im aktuellen Monat nicht gibt, so wird der letzte Tag des Monats verwendet. Beispiel: Ein Zeitplan der monatlich am 31. Tag ausgeführt werden soll, wird im April am 30. ausgeführt. Im Februar wird der Zeitplan am 28. (am 29. in Schaltjahren) ausgeführt. • **jährlich**: Der Zeitplan soll in einem definierten Intervall von Jahren, an bestimmten Tagen, zu definierten Uhrzeiten ausgeführt werden, beispielsweise jedes Jahr am 1.Tag, am 100. Tag und am 200.Tag jeweils um 6:00 Uhr und um 18:00 Uhr. • Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll. • Legen Sie unter **Wiederholen alle** fest, nach wie vielen Jahren der Zeitplan wiederholt werden soll. • Legen Sie die Tage des Jahres fest (1. bis 366.Tag eines Jahres). HINWEIS: Wenn der 366. Tag des Jahres gewählt wird, wird der Zeitplan nur in Schaltjahren ausgeführt.

Eigenschaft	Bedeutung
	• **Montag**, **Dienstag**, **Mittwoch**, **Donnerstag**, **Freitag**, **Samstag**, **Sonntag**: Der Zeitplan soll an einem bestimmten Wochentag, in definierten Monaten, zu definierten Uhrzeiten ausgeführt werden, beispielsweise am zweiten Samstag im Januar und im Juni um 10:00 Uhr. • Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll. • Legen Sie unter **Wiederholen alle** fest, am wievielten Wochentag eines Monats der Zeitplan ausgeführt werden soll. Zulässig sind die Werte **1** bis **4**, **-1** (letzter entsprechender Wochentag) und **-2** (vorletzter entsprechender Wochentag). • Legen Sie den Monat fest, in welchem der Zeitplan ausgeführt werden soll. Zulässig sind die Werte **1** bis **12**. Ist der Wert leer, wird der Zeitplan in jedem Monat ausgeführt.
Startzeit	Feste Startzeit. Geben Sie die Uhrzeit in der Ortszeit der ausgewählten Zeitzone an. Bei einer Liste von Startzeiten wird der Zeitplan zu jeder dieser Zeiten gestartet.
Wiederholen alle	Ausführungsfrequenz, mit welcher der zeitgesteuerte Auftrag innerhalb des gewählten Zeitintervalls ausgeführt werden soll.

Verwandte Themen

- Dynamische Rollen an Zeitpläne zuweisen auf Seite 47
- Zeitpläne für dynamische Rollen sofort ausführen auf Seite 46
- Stammdaten für dynamische Rollen auf Seite 53

Zeitpläne für dynamische Rollen sofort ausführen

HINWEIS: Wenn ein Zeitplan gestartet wird, werden Neuberechnungen für alle dynamischen Rollen ausgeführt, denen der Zeitplan zugeordnet ist und für die die Option **Keine Neuberechnung von Zuweisungen** nicht aktiviert ist.

Um einen Zeitplan sofort zu starten

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Sofort ausführen**.

   Es erscheint eine Meldung, die bestätigt, dass der Zeitplan gestartet wurde.

Dynamische Rollen an Zeitpläne zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Zeitplan die dynamischen Rollen zu, die mit diesem Zeitplan ausgeführt werden sollen. Auf dem Zuordnungsformular werden alle dynamischen Rollen angezeigt, denen der ausgewählte Zeitplan zugewiesen ist.

Um dynamische Rollen an einen Zeitplan zuzuweisen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Dynamische Rollen zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die dynamischen Rollen, die zugewiesen werden sollen.
5. Speichern Sie die Änderungen.

Um eine Zuordnung zu ändern

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Dynamische Rollen zuweisen**.
4. Wählen Sie im Kontextmenü des Zuordnungsformulars **Zeige bereits anderen Objekten zugewiesene Objekte**.

   Es werden die dynamischen Rollen eingeblendet, die bereits anderen Zeitplänen zugewiesen sind.
5. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf eine dieser dynamischen Rollen.

   Dieser dynamischen Rolle wird der aktuell ausgewählte Zeitplan zugeordnet.
6. Speichern Sie die Änderungen.

HINWEIS: Zuordnungen können nicht entfernt werden. Die Zuordnung eines Zeitplans ist für dynamische Rollen eine Pflichteingabe.

Verwandte Themen

- Stammdaten für dynamische Rollen auf Seite 53

Dynamische Rollen bei Änderungen von Objekten sofort berechnen

Die Rollenmitgliedschaften können bei Eigenschaftsänderung der Objekte sofort durch den DBQueue Prozessor überprüft und nötigenfalls geändert. Sie können für jede dynamische

Rollen festlegen, bei welchen Eigenschaften eine erneute Berechnung der Rollenmitgliedschaften erfolgen soll.

Voraussetzungen für die sofortige Neuberechnung

- Die Konfigurationsparameter für die sofortige Neuberechnung sind aktiviert. Prüfen Sie im Designer die folgenden Konfigurationsparameter und aktivieren Sie diese bei Bedarf.
  - **QER | Structures | DynamicGroupCheck**: Der Konfigurationsparameter steuert die Erzeugung von Berechnungsaufträgen für dynamische Rollen.

    Ist der Konfigurationsparameter deaktiviert, sind auch die untergeordneten Konfigurationsparameter nicht wirksam.
  - **QER | Structures | DynamicGroupCheck | CalculateImmediatelyPerson**: Ist der Konfigurationsparameter aktiviert, wird bei Änderungen an Personen oder Personen-nahen Objekten sofort ein Berechnungsauftrag für den DBQueue Prozessor eingestellt.
  - **QER | Structures | DynamicGroupCheck | CalculateImmediatelyHardware**: Ist der Konfigurationsparameter aktiviert, wird bei Änderungen an Geräten oder Geräte-nahen Objekten sofort ein Berechnungsauftrag für den DBQueue Prozessor eingestellt.
  - **QER | Structures | DynamicGroupCheck | CalculateImmediatelyWorkdesk**: Ist der Konfigurationsparameter aktiviert, wird bei Änderungen an Arbeitsplätzen oder Arbeitsplatz-nahen Objekten sofort ein Berechnungsauftrag für den DBQueue Prozessor eingestellt.
- Für die dynamischen Rollen ist die Option **Sofortige Neuberechnung der Zuweisungen** aktiviert. Es sind die Eigenschaften definiert, die eine Neuberechnung auslösen sollen.
- Für die dynamischen Rollen ist die Option **Keine Neuberechnung von Zuweisungen** nicht aktiviert.

Um die sofortige Neuberechnung für eine dynamische Rolle zu aktivieren

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Aktivieren Sie die Option **Sofortige Neuberechnung der Zuweisungen**.
6. Auf dem Tabreiter **Neuberechnungseigenschaften** fügen Sie die Eigenschaften ein, die eine erneute Berechnung der dynamischen Rolle auslösen sollen.
   a. Klicken Sie **Hinzufügen**.
   b. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld **Eigenschaft**.

c. Wählen Sie unter **Eigenschaft** die Tabelle und Spalte, die eine erneute Berechnung auslösen soll.

d. Klicken Sie **OK**.

e. Wiederholen Sie diese Schritte für alle Eigenschaften.

7. Speichern Sie die Änderungen.

Verwandte Themen

- Eigenschaften für die sofortige Neuberechnung bearbeiten auf Seite 49
- Stammdaten für dynamische Rollen auf Seite 53
- Berechnung der Rollenmitgliedschaften für dynamische Rollen auf Seite 41
- Rollenmitgliedschaften für dynamische Rollen sofort berechnen auf Seite 50

Eigenschaften für die sofortige Neuberechnung bearbeiten

Sie können für einzelne dynamische Rollen festlegen, bei welchen Eigenschaften eine erneute Berechnung der Rollenmitgliedschaften erfolgen soll.

Um eine Eigenschaft hinzuzufügen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Fügen Sie auf dem Tabreiter **Neuberechnungseigenschaften** die Eigenschaften hinzu.

   a. Klicken Sie **Hinzufügen**.

   b. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld **Eigenschaft**.

   c. Wählen Sie unter **Eigenschaft** die Tabelle und Spalte, die eine erneute Berechnung auslösen soll.

   d. Klicken Sie **OK**.

6. Speichern Sie die Änderungen.

Um eine Eigenschaft zu deaktivieren

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.

3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Neuberechnungseigenschaften** die Spalte in der Liste aus und aktivieren Sie die Option **deaktiviert**.
6. Speichern Sie die Änderungen.

Um eine Eigenschaft zu entfernen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Neuberechnungseigenschaften** die Spalte in der Liste aus und klicken Sie **Entfernen**.
6. Speichern Sie die Änderungen.

Rollenmitgliedschaften für dynamische Rollen sofort berechnen

Sie können die Berechnung für eine einzelne dynamische Rolle auch sofort ausführen.

Um Rollenmitgliedschaften sofort zu berechnen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie die Aufgabe **Neuberechnung sofort veranlassen** und schließen Sie die Meldung mit **OK**.

   Es wird ein Verarbeitungsauftrag für den DBQueue Prozessor in die DBQueue eingestellt.

Verwandte Themen

- Berechnung der Rollenmitgliedschaften für dynamische Rollen auf Seite 41
- Dynamische Rollen bei Änderungen von Objekten sofort berechnen auf Seite 47
- Eigenschaften für die sofortige Neuberechnung bearbeiten auf Seite 49

Dynamische Rollen von der Neuberechnung ausschließen

Einzelne dynamische Rollen können Sie von der Neuberechnung ausschließen. In diesem Fall werden die Rollenmitgliedschaften nicht automatisch neu berechnet. Bereits bestehende Rollenmitgliedschaften bleiben bestehen.

Um eine dynamische Rolle von der Neuberechnung auszuschließen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Aktivieren Sie die Option **Keine Neuberechnung von Zuweisungen**.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Berechnung der Rollenmitgliedschaften für dynamische Rollen auf Seite 41
- Stammdaten für dynamische Rollen auf Seite 53

Personen aus dynamischen Rollen ausschließen

Personen können aufgrund einer abgelehnten Attestierung oder einer Regelverletzung automatisch aus dynamischen Rollen ausgeschlossen werden. Dafür wird eine Ausschlussliste geführt. Zusätzlich können Ausschlüsse auch direkt für einzelne Personen definiert werden.

Um eine Person in die Ausschlussliste aufzunehmen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für diese Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Personen ausschließen**.
5. Klicken Sie **Hinzufügen** und wählen Sie die Person aus der Auswahlliste **Person** aus.
6. (Optional) Erfassen Sie eine Begründung für den Ausschluss.
7. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten der Ausschlussliste für dynamische Rollen auf Seite 52
- Personen aus der Ausschlussliste entfernen auf Seite 52
- Dynamische Rollen mit fehlerhaft ausgeschlossenen Personen auf Seite 92

Personen aus der Ausschlussliste entfernen

Um eine Person aus der Ausschlussliste zu entfernen

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde.
2. Öffnen Sie das Überblicksformular für diese Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Personen ausschließen**.
5. Wählen Sie die Person und klicken Sie **Entfernen**.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten der Ausschlussliste für dynamische Rollen auf Seite 52
- Personen aus dynamischen Rollen ausschließen auf Seite 51

Stammdaten der Ausschlussliste für dynamische Rollen

Für eine Person in der Ausschlussliste einer dynamischen Rolle werden folgende Stammdaten angezeigt.

Tabelle 6: Stammdaten der Ausschlussliste für dynamische Rollen

Eigenschaft	Beschreibung
Person	Eindeutige Kennung der ausgeschlossenen Person.
Beschreibung	Begründung für den Ausschluss der Person. Wenn die Person aufgrund einer abgelehnten Attestierung oder einer Regelverletzung ausgeschlossen wurde, ist hier eine Standardbegründung eingetragen.
Bedingung nicht zutreffend	Gibt an, ob die Bedingung der dynamischen Rolle auf die ausgeschlossene Person zutrifft. Wenn die Option deaktiviert ist, trifft die Bedingung zu.

Eigenschaft	Beschreibung
	TIPP: Wenn die Option aktiviert ist, kann die Person aus der Ausschlussliste entfernt werden. Weitere Informationen finden Sie unter Personen aus der Ausschlussliste entfernen auf Seite 52.
Nicht durch dynamische Rolle zugewiesen	Gibt an, ob die ausgeschlossene Person noch über einen anderen Weg an die Rolle zugewiesen ist. Personen können zusätzlich auch direkt oder durch eine Zuweisungsbestellung oder Delegierung Mitglied der Rolle werden. Auf diese Zuweisungen hat die Ausschlussliste keinen Einfluss.

Verwandte Themen

- Personen aus dynamischen Rollen ausschließen auf Seite 51
- Personen aus der Ausschlussliste entfernen auf Seite 52
- Dynamische Rollen mit fehlerhaft ausgeschlossenen Personen auf Seite 92

Überblick über dynamische Rollen anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Information zu einer dynamischen Rolle.

Um einen Überblick über eine dynamische Rolle zu erhalten

1. Wählen Sie im Manager die Rolle, für die eine dynamische Rolle erstellt wurde, beispielsweise die Abteilung.
2. Öffnen Sie das Überblicksformular für die Rolle.
3. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
4. Wählen Sie die Aufgabe **Überblick über die dynamische Rolle**.
5. Wählen Sie den Bericht **Übersicht anzeigen**.

   Der Bericht enthält eine Zusammenfassung der wichtigsten Information zu einer dynamischen Rolle einschließlich des Zeitplans, der ausgeschlossenen Personen und der Eigenschaften zur Neuberechnung.

Stammdaten für dynamische Rollen

Für eine dynamische Rolle erfassen Sie die folgenden Daten.

Tabelle 7: Stammdaten einer dynamischen Rolle

Eigenschaft	Beschreibung
Rolle/Organisation	Rolle (Abteilung, Kostenstelle, Standort, Geschäftsrolle, IT Shop Knoten, Anwendungsrolle), auf welche die dynamische Rolle verweist. Diese Angabe ist mit der ausgewählten Rolle vorbelegt.
Objektklasse	Objektklasse, für welche die dynamische Rolle gelten soll. Wählen Sie zwischen **Person**, **Hardware** und **Workdesk**. HINWEIS: Die Kombination aus Objektklasse und Rolle muss eindeutig sein. Es ist nicht möglich, das zwei dynamische Rollen einer Objektklasse auf eine Rolle verweisen.
Dynamische Rolle	Bezeichnung der dynamischen Rolle.
Zeitplan der Berechnung	Zeitplan, durch den die zyklische Neuberechnung der Rollenmitgliedschaft ausgelöst wird. Um einen neuen Zeitplan zu erstellen, klicken Sie . Erfassen Sie die Stammdaten für den Zeitplan.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bedingung	Definiert, welche Objekte der Objektklasse Mitglieder der ausgewählten Rolle werden. Weitere Informationen finden Sie unter Hinweise zu Bedingungen für dynamische Rollen auf Seite 39. Weitere Informationen finden Sie unter Hinweise zu Bedingungen für dynamische Rollen auf Seite 39.
Keine Neuberechnung von Zuweisungen	Gibt an, ob eine Neuberechnung von Mitgliedschaften erfolgen soll. Ist die Option aktiviert, werden die Rollenmitgliedschaften nicht automatisch neu berechnet. Bereits bestehende Rollenmitgliedschaften bleiben bestehen.
Sofortige Neuberechnung von Zuweisungen	Gibt an, ob bei Änderung der festgelegten Eigenschaften eine Neuberechnung der dynamischen Rolle erfolgt. Wenn die Option aktiviert ist, legen Sie die Eigenschaften für die Neuberechnung fest.
Neuberechnungseigenschaft: Eigenschaft	Eigenschaft, deren Änderung eine sofortige Neuberechnung der dynamischen Rolle auslöst.
Neuberechnungseigenschaft: Deaktiviert	Gibt an, ob die sofortige Neuberechnung der Eigenschaft deaktiviert ist.

Verwandte Themen

- Dynamische Rollen erstellen und bearbeiten auf Seite 38
- Bedingungen für dynamische Rollen testen auf Seite 41
- Zeitpläne zur Berechnung von dynamischen Rollen auf Seite 42
- Dynamische Rollen an Zeitpläne zuweisen auf Seite 47
- Rollenmitgliedschaften für dynamische Rollen sofort berechnen auf Seite 50
- Dynamische Rollen von der Neuberechnung ausschließen auf Seite 51

Abteilungen, Kostenstellen und Standorte

Aufgrund ihrer besonderen Bedeutung für betriebliche Abläufe in vielen Unternehmen werden Abteilungen, Kostenstellen und Standorte in eigenständigen Hierarchien, unter dem Begriff **Organisationen** abgebildet. An Organisationen können verschiedene Unternehmensressourcen zugewiesen werden, beispielsweise Berechtigungen in SAP Systemen oder Azure Active Directory Mandanten. Personen können als Mitglieder in die einzelnen Rollen aufgenommen werden. Bei entsprechender Konfiguration des One Identity Manager erhalten die Personen über diese Zuordnungen ihre Unternehmensressourcen.

Detaillierte Informationen zum Thema

- Zusatzeigenschaften an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 95
- Berichte über Abteilungen, Kostenstellen und Standorte auf Seite 97
- Konfigurationsparameter für die Verwaltung von Abteilungen, Kostenstellen und Standorten auf Seite 227

One Identity Manager Benutzer für die Verwaltung von Abteilungen, Kostenstellen und Standorten

In die Verwaltung von Abteilungen, Kostenstellen und Standorte sind folgende Benutzer eingebunden.

Tabelle 8: Benutzer

Benutzer	Aufgaben
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen und Bearbeiten die Abteilungen, Kostenstellen und Standorte. • Weisen Unternehmensressourcen an die Abteilungen, Kostenstellen und Standorte zu. • Attestieren die Stammdaten von Abteilungen, Kostenstellen und Standorten. • Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
Zusätzliche Manager	Die zusätzlichen Manager müssen der Anwendungsrolle **Identity Management | Organisationen | Zusätzliche Manager** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind berechtigt Abteilungen, Kostenstellen und Standorte zu verwalten.
Attestierer für Organisationen	Die Attestierer müssen der Anwendungsrolle **Identity Management | Organisationen | Attestierer** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Abteilungen, Kostenstellen und Standorte, für die sie verantwortlich sind. • Können die Stammdaten der Abteilungen, Kostenstellen und Standorte sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Genehmiger für Organisationen	Die Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind Genehmiger für den IT Shop. • Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.
Genehmiger (IT) für Organisationen	Die IT Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger (IT)** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind IT Genehmiger für den IT Shop. • Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Basisdaten für Abteilungen, Kostenstellen und Standorte

Für die Abbildung von hierarchischen Rollen 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**.

- Rollenklassen

  Rollenklassen bilden die Basis für die Abbildung von hierarchischen Rollen im One Identity Manager. Rollenklassen dienen zur Zusammenfassung gleichartiger Rollen.

- Rollentypen

  Zur Einteilung von Rollen erstellen Sie Rollentypen. Rollentypen werden beispielsweise zur Abbildung der Rollen in der Benutzeroberfläche genutzt.

- Unternehmensbereiche

  Um Regelprüfungen im Rahmen des Identity Audit für verschiedene Bereiche Ihres Unternehmens auswerten zu können, richten Sie Unternehmensbereiche ein. Unternehmensbereiche können an Rollen zugeordnet werden. Für Unternehmensbereiche und Rollen können Sie Kriterien erfassen, die Auskunft über das Risiko von Regelverletzungen geben. Unternehmensbereiche können darüber hinaus bei der Peer-Gruppen-Analyse von Bestellungen oder Attestierungsvorgängen genutzt werden.

- Attestierer

  Im One Identity Manager können Sie an Abteilungen, Kostenstellen und Standorte Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows für die Attestierungsvorgänge als verantwortliche Attestierer herangezogen werden. Dazu ordnen Sie den Abteilungen, Kostenstellen und Standorten eine Anwendungsrolle für Attestierer zu. Ausführliche Informationen zur Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

  Im One Identity Manager ist eine Standardanwendungsrolle für Attestierer vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

- Genehmiger und Genehmiger (IT)

Im One Identity Manager können Sie an Abteilungen, Kostenstellen und Standorte Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows als verantwortliche Entscheider für Genehmigungsverfahren bei IT Shop-Bestellungen herangezogen werden. Dazu ordnen Sie den Abteilungen, Kostenstellen und Standorten Anwendungsrollen für Genehmiger zu. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Im One Identity Manager sind Standardanwendungsrollen für Genehmiger und Genehmiger (IT) vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Detaillierte Informationen zum Thema

- Rollenklassen für Abteilungen, Kostenstellen und Standorte auf Seite 60
- Rollentypen für Abteilungen, Kostenstellen und Standorte auf Seite 61
- Unternehmensbereiche für Abteilungen, Kostenstellen und Standorte auf Seite 63
- Attestierer für Abteilungen, Kostenstellen und Standorte auf Seite 65
- Genehmiger und Genehmiger (IT) für Abteilungen, Kostenstellen und Standorte auf Seite 66
- Konfigurationsparameter für die Verwaltung von Abteilungen, Kostenstellen und Standorten auf Seite 227

Rollenklassen für Abteilungen, Kostenstellen und Standorte

Rollenklassen bilden die Basis für die Abbildung von hierarchischen Rollen im One Identity Manager. Rollenklassen dienen zur Zusammenfassung gleichartiger Rollen. An der Rollenklasse ist die Vererbungsrichtung festgelegt. Zusätzlich wird für eine Rollenklasse festgelegt, welche Zuweisungen an die einzelnen Rollen dieser Rollenklasse erlaubt sind.

Folgende Rollenklassen sind standardmäßig für die Abbildung von Organisationen im One Identity Manager vorhanden:

- Abteilung
- Kostenstelle
- Standort

Für Abteilungen, Kostenstellen, Standorte und Anwendungsrollen ist eine Top-Down Vererbung definiert. Für Abteilungen, Kostenstellen und Standorte sind Zuweisungen von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen vordefiniert. Sie können diese Zuweisungen für eine Rollenklasse bearbeiten.

Verwandte Themen

- Vererbungsrichtungen innerhalb einer Hierarchie auf Seite 12
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Rollentypen an Rollenklassen für Abteilungen, Kostenstellen und Standorte zuweisen

Um Rollentypen an eine Rollenklasse zuzuweisen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen**.
2. Wählen Sie in der Ergebnisliste die Rollenklasse.
3. Wählen Sie die Aufgabe **Rollentyp zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollentypen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Rollentyp und doppelklicken Sie ✓.

Verwandte Themen

- Rollentypen für Abteilungen, Kostenstellen und Standorte auf Seite 61
- Rollentypen für Abteilungen, Kostenstellen und Standorte erstellen auf Seite 62
- Rollenklassen an Rollentypen für Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 63

Rollentypen für Abteilungen, Kostenstellen und Standorte

Zur weiteren Klassifizierung können Sie Rollentypen definieren und an Rollenklassen und an Rollen zuweisen. Dabei gelten folgende Einschränkungen:

- Einen Rollentyp können Sie an mehrere Rollenklassen zuweisen.
- Wenn Sie einer Rollenklasse Rollentypen zuweisen, dann können Sie an den Rollen dieser Rollenklasse nur diese Rollentypen auswählen. Andere Rollentypen werden nicht zur Auswahl angeboten.

- Wenn Sie einer Rollenklasse keinen Rollentyp zuweisen, dann können Sie an den Rollen dieser Rollenklasse nur die Rollentypen verwenden, die keiner anderen Rollenklasse zugewiesen sind.
- Der Rollentyp **Geschäftsrollen** ist vordefiniert. Dieser Rollentyp kann nicht an die Rollenklassen **Abteilung**, **Kostenstelle** oder **Standort** zugewiesen werden. Weisen Sie diesen Rollentyp an die Rollenklassen zu, die Geschäftsrollen abbilden.

Beispiel:

Rollentyp **Geschäftsrollen** ist vordefiniert. Es werden zusätzlich die Rollentypen **Region**, **Land**, **Vertrieb** und **Entwicklung** erstellt.

- Der Rollenklasse **Externe Projekte** wird der Rollentyp **Geschäftsrollen** zugewiesen.

  Rollen dieser Rollenklasse können den Rollentyp **Geschäftsrollen** erhalten.
- Der Rollenklasse **Mitarbeiter** werden die Rollentypen **Geschäftsrolle**, **Region** und **Land** zugewiesen.

  Rollen diese Rollenklasse können die Rollentypen **Geschäftsrolle**, **Region** und **Land** erhalten.
- Der Rollenklasse **Standort** werden die Rollentypen **Region** und **Land** zugewiesen.

  Standorte können die Rollentypen **Region** und **Land** erhalten.
- Den Rollenklassen **Kostenstelle** und **Abteilung** werden keine Rollentypen zugewiesen.

  Kostenstellen und Abteilungen können die Rollentypen **Vertrieb** und **Entwicklung** erhalten.

Rollentypen für Abteilungen, Kostenstellen und Standorte erstellen

Um Rollentypen zu erstellen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollentypen**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die folgenden Informationen:
   - **Rollentyp**: Bezeichnung des Rollentyp. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
   - **Beschreibung**: (Optional) Freitextfeld für zusätzliche Erläuterungen.

- **Keine Mehrfachzuweisung von Personen**: Die Option wirkt nicht für Abteilungen, Kostenstellen und Standorte.

4. Speichern Sie die Änderungen.

Rollenklassen an Rollentypen für Abteilungen, Kostenstellen und Standorte zuweisen

Um Rollenklassen an einen Rollentyp zuzuweisen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollentypen**.
2. Wählen Sie in der Ergebnisliste den Rollentyp.
3. Wählen Sie die Aufgabe **Rollenklassen 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

- Rollentypen für Abteilungen, Kostenstellen und Standorte auf Seite 61
- Rollentypen an Rollenklassen für Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 61

Unternehmensbereiche für Abteilungen, Kostenstellen und Standorte

Um Regelprüfungen im Rahmen des Identity Audit für verschiedene Bereiche Ihres Unternehmens auswerten zu können, richten Sie Unternehmensbereiche ein. Unternehmensbereiche können an hierarchische Rollen und Leistungspositionen zugeordnet werden. Für die Unternehmensbereiche und die hierarchischen Rollen können Sie Kriterien erfassen, die Auskunft über das Risiko von Regelverletzungen geben. Dafür legen Sie fest, wie viele Regelverletzungen in einem Unternehmensbereich oder einer Rolle

zulässig sind. Für jede Rolle können Sie separate Bewertungskriterien erfassen, wie beispielsweise Risikoindex oder Transparenzindex.

Unternehmensbereiche können darüber hinaus bei der Entscheidung von Bestellungen oder Attestierungsvorgängen durch Peer-Gruppen-Analyse genutzt werden.

Beispiel: Einsatz von Unternehmensbereichen

Das Risiko von Regelverletzungen für Kostenstellen soll bewertet werden. Gehen Sie folgendermaßen vor:

1. Richten Sie Unternehmensbereiche ein.
2. Ordnen Sie die Unternehmensbereiche den Kostenstellen zu.
3. Definieren Sie Bewertungskriterien für die Kostenstellen.
4. Legen Sie die Anzahl zulässiger Regelverletzungen für die Unternehmensbereiche fest.
5. Weisen Sie die Unternehmensbereiche den Complianceregeln zu, die für die Auswertung relevant sind.
6. Erstellen Sie über die Berichtsfunktion des One Identity Manager einen Bericht, der das Ergebnis der Regelprüfung für die Unternehmensbereiche nach beliebigen Kriterien aufbereitet.

Um Unternehmensbereiche zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Unternehmensbereiche**.
2. Wählen Sie in der Ergebnisliste einen Unternehmensbereich und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Für einen Unternehmensbereich erfassen Sie folgende Stammdaten.

Tabelle 9: Eigenschaften von Unternehmensbereichen

Eigenschaft	Beschreibung
Unternehmensbereich	Bezeichnung des Unternehmensbereichs.
Überg. Unternehmensbereich	Übergeordneter Unternehmensbereich in einer Hierarchie. Wählen Sie aus der Auswahlliste den übergeordneten Unternehmensbereich aus, um Unternehmensbereiche hierarchisch zu organisieren.

Eigenschaft	Beschreibung
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in diesem Unternehmensbereich zulässig sind. Dieser Wert kann bei der Regelprüfung ausgewertet werden. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Complianceregeln vorhanden ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Ausführliche Informationen zur Regelprüfung finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln*. Ausführliche Informationen zur Peer-Gruppen-Analyse finden Sie im *One Identity Manager Administrationshandbuch für IT Shop* und im *One Identity Manager Administrationshandbuch für Attestierungen*.

Attestierer für Abteilungen, Kostenstellen und Standorte

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

Im One Identity Manager können Sie an Abteilungen, Kostenstellen und Standorte Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows für die Attestierungsvorgänge als verantwortliche Attestierer herangezogen werden. Dazu ordnen Sie den Abteilungen, Kostenstellen und Standorten eine Anwendungsrolle für Attestierer zu. Ausführliche Informationen zur Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Im One Identity Manager ist eine Standardanwendungsrolle für Attestierer vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 10: Standardanwendungsrolle für Attestierer

Benutzer	Aufgaben
Attestierer für Organisationen	Die Attestierer müssen der Anwendungsrolle **Identity Management | Organisationen | Attestierer** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Abteilungen, Kostenstellen und Standorte, für die sie verantwortlich sind. • Können die Stammdaten der Abteilungen, Kostenstellen und Standorte sehen, aber nicht bearbeiten.

Benutzer	Aufgaben
	HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Um Personen in die Standardanwendungsrolle für Attestierer aufzunehmen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Attestierer**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. 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 .
4. Speichern Sie die Änderungen.

Genehmiger und Genehmiger (IT) für Abteilungen, Kostenstellen und Standorte

Im One Identity Manager können Sie an Abteilungen, Kostenstellen und Standorte Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows als verantwortliche Entscheider für Genehmigungsverfahren bei IT Shop-Bestellungen herangezogen werden. Dazu ordnen Sie den Abteilungen, Kostenstellen und Standorten Anwendungsrollen für Genehmiger zu. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Im One Identity Manager sind Standardanwendungsrollen für Genehmiger und Genehmiger (IT) vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 11: Standardanwendungsrollen für Genehmiger

Benutzer	Aufgaben
Genehmiger für Organisationen	Die Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind Genehmiger für den IT Shop. • Entscheiden über Bestellungen aus Abteilungen, Kostenstellen

Benutzer	Aufgaben
	und Standorten, für die sie verantwortlich sind.
Genehmiger (IT) für Organisationen	Die IT Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger (IT)** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind IT Genehmiger für den IT Shop. • Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.

Um Genehmiger oder Genehmiger (IT) festzulegen

1. Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Genehmiger**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen > Basisdaten zur Konfiguration > Genehmiger (IT)**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. 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 .
4. Speichern Sie die Änderungen.

Abteilungen erstellen und bearbeiten

Um eine Abteilung zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen**.
2. Wählen Sie in der Ergebnisliste eine Abteilung und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Abteilungen auf Seite 68
- Kontaktinformationen für Abteilungen auf Seite 71
- Unternehmensbereich und Risikobewertung für Abteilungen auf Seite 71
- IT Betriebsdaten für Abteilungen, Kostenstellen und Standorte einrichten auf Seite 82

Allgemeine Stammdaten für Abteilungen

Für eine Abteilung erfassen Sie die folgenden allgemeine Stammdaten.

Tabelle 12: Allgemeine Stammdaten einer Abteilung

Eigenschaft	Beschreibung
Abteilung	Bezeichnung der Abteilung. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Kurzname	Kurzbezeichnung der Abteilung.
Objekt ID	Eindeutige Objekt-ID der Abteilung. Die Objekt-ID wird beispielsweise in SAP Systemen zur Zuordnung von Mitarbeitern zu Abteilungen benötigt.
Übergeordnete Abteilung	Übergeordnete Abteilung in der Rollenhierarchie. Um Abteilungen hierarchisch zu organisieren, wählen Sie in der Auswahlliste die übergeordnete Abteilung aus. Für eine Abteilung, die in der obersten Ebene einer Abteilungshierarchie steht, lassen Sie dieses Eingabefeld leer.
Vollständiger Name	Kompletter Name der Abteilung einschließlich übergeordneter Abteilungen. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Rollentyp	Rollentyp zur weiteren Klassifizierung.
Standort	Standort, dem die Abteilung primär zugeordnet ist.
Manager	Verantwortlicher Manager der Abteilung.
2. Verantwortlicher	Stellvertretender Manager der Abteilung.
Zusätzliche Manager	Anwendungsrolle für eine Gruppe von Managern und Stellvertretern, die diese Abteilung verwalten. Um eine neue Anwendungsrolle zu erstellen, klicken Sie. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.

Eigenschaft	Beschreibung
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge für die Abteilung zu entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Kostenstelle	Kostenstelle, der die Abteilung primär zugeordnet ist.
Genehmiger	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieser Abteilung entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Genehmiger (IT)	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieser Abteilung entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Zertifizierungsstatus	Zertifizierungsstatus der Abteilung. Folgende Zertifizierungsstatus können ausgewählt werden: • **Neu**: Die Abteilung wurde neu in der One Identity Manager-Datenbank angelegt. • **Zertifiziert**: Die Stammdaten der Abteilung wurden durch einen Manager genehmigt. • **Abgelehnt**: Die Stammdaten der Abteilung wurden durch einen Manager nicht genehmigt. Der Zertifizierungsstatus kann abhängig vom Ergebnis regelmäßiger Attestierungen gesetzt werden.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Vollständiger Name	Vollständige Bezeichnung der Abteilung inklusive der übergeordneten Abteilungen.
Deaktiviert	Gibt an, ob die Abteilung aktiv genutzt wird. Aktivieren Sie diese

Eigenschaft	Beschreibung
	Option, wenn die Abteilung nicht genutzt wird. Die Option hat keinen Einfluss auf die Berechnung der Vererbung.
Vererbung blockieren	Gibt an, ob die Vererbung an dieser Abteilung unterbrochen wird. Aktivieren Sie diese Option, um die Vererbung innerhalb der Abteilungshierarchie zu unterbrechen.
X500 Knoten	Aktivieren Sie diese Option, um die Abteilung für den Export in ein X500-Schema zu kennzeichnen.
Keine Vererbung an Personen	Gibt an, ob die Vererbung an Personen für die Abteilung vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Gibt an, ob die Vererbung an Geräte für die Abteilung vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Gibt an, ob die Vererbung an Arbeitsplätze für die Abteilung vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Gibt an, ob für die Abteilung eine dynamische Rolle erstellt werden darf.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01 ... Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Rollentypen für Abteilungen, Kostenstellen und Standorte auf Seite 61
- Attestierer für Abteilungen, Kostenstellen und Standorte auf Seite 65
- Genehmiger und Genehmiger (IT) für Abteilungen, Kostenstellen und Standorte auf Seite 66
- Vererbung über Rollen blockieren auf Seite 32
- Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern auf Seite 33
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten auf Seite 91
- Zertifizierung von Abteilungen, Kostenstellen und Standorten auf Seite 96

Kontaktinformationen für Abteilungen

Für Abteilungen erfassen Sie die folgenden Kontaktinformationen. Über die Schaltfläche neben dem Eingabefeld schalten Sie die Eingabe frei und können Einträge hinzufügen. Über die Schaltfläche können Sie Einträge aus einer Auswahlliste entfernen.

Tabelle 13: Kontaktinformationen einer Abteilung

Eigenschaft	Beschreibung
E-Mail-Adressen	E-Mail-Adressen der Abteilung.
Besuchsadressen	Besuchsadressen der Abteilung.
Besuchszeiten	Besuchszeiten der Abteilung.
Telefonzeiten	Telefonzeiten der Abteilung.
Geschäftszeiten	Geschäftszeiten der Abteilung.
Postleitzahl	Postleitzahl der Abteilung.

Unternehmensbereich und Risikobewertung für Abteilungen

Für die Risikobewertung einer Abteilung im Rahmen des Identity Audits können Sie hier Werte für die Einstufung der Abteilung erfassen.

Tabelle 14: Stammdaten zum Unternehmensbereich einer Abteilung

Eigenschaft	Beschreibung
Land	Land. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln.
Bundesland	Bundesland. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln.
Unternehmensbereich	Unternehmensbereich der Abteilung. Die Angabe wird zur Risikobewertung der Abteilung benötigt.
Risikoindex (berechnet)	Für die Risikobewertung der Abteilung wird anhand der zugewiesenen Unternehmensressourcen ein Risikoindex berechnet. 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.*

Eigenschaft	Beschreibung
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen an die Abteilung sind. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein. **0**: keine Transparenz **1**: volle Transparenz
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in dieser Abteilung zulässig sind. Der Wert kann bei der Prüfung von Complianceregeln ausgewertet werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln.* HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Complianceregeln vorhanden ist.
Umsatz des Bereichs	Umsatz der Abteilung.
Gewinn des Bereichs	Gewinn der Abteilung.

Verwandte Themen

- Ermitteln der Sprache für Personen auf Seite 161
- Ermitteln der Arbeitszeiten für Personen auf Seite 162
- Unternehmensbereiche für Abteilungen, Kostenstellen und Standorte auf Seite 63

Kostenstellen erstellen und bearbeiten

Um eine Kostenstelle zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Organisationen > Kostenstellen**.
2. Wählen Sie in der Ergebnisliste eine Kostenstelle und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kostenstellen auf Seite 73
- Unternehmensbereich und Risikobewertung für Kostenstellen auf Seite 75

- IT Betriebsdaten für Abteilungen, Kostenstellen und Standorte einrichten auf Seite 82

Allgemeine Stammdaten für Kostenstellen

Für eine Kostenstelle erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 15: Allgemeine Stammdaten einer Kostenstelle

Eigenschaft	Beschreibung
Kostenstelle	Bezeichnung der Kostenstelle. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Kurzname	Kurzbezeichnung der Kostenstelle.
Übergeordnete Kostenstelle	Übergeordnete Kostenstelle in der Rollenhierarchie. Um Kostenstellen hierarchisch zu organisieren, wählen Sie in der Auswahlliste die übergeordnete Kostenstelle aus. Für eine Kostenstelle, die in der obersten Ebene einer Kostenstellenhierarchie steht, lassen Sie dieses Eingabefeld leer.
Vollständiger Name	Kompletter Name der Kostenstelle einschließlich übergeordneter Kostenstellen. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Rollentyp	Rollentyp zur weiteren Klassifizierung.
Manager	Verantwortlicher Manager der Kostenstelle.
2. Verantwortlicher	Stellvertretender Manager der Kostenstelle.
Zusätzliche Manager	Anwendungsrolle für eine Gruppe von Managern und Stellvertretern, die diese Kostenstelle verwalten. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge für die Kostenstelle zu entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Abteilung	Abteilung, der die Kostenstelle primär zugeordnet ist.
Standort	Standort, dem die Kostenstelle primär zugeordnet ist.

Eigenschaft	Beschreibung
Genehmiger	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieser Kostenstelle entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Genehmiger (IT)	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieser Kostenstelle entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Zertifizierungsstatus	Zertifizierungsstatus der Kostenstelle. Folgende Zertifizierungsstatus können ausgewählt werden: • **Neu**: Die Kostenstelle wurde neu in der One Identity Manager-Datenbank angelegt. • **Zertifiziert**: Die Stammdaten der Kostenstelle wurden durch einen Manager genehmigt. • **Abgelehnt**: Die Stammdaten der Kostenstelle wurden durch einen Manager nicht genehmigt. Der Zertifizierungsstatus kann abhängig vom Ergebnis regelmäßiger Attestierungen gesetzt werden.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Deaktiviert	Gibt an, ob die Kostenstelle aktiv genutzt wird. Aktivieren Sie diese Option, wenn die Kostenstelle nicht genutzt wird. Die Option hat keinen Einfluss auf die Berechnung der Vererbung.
Vererbung blockieren	Gibt an, ob die Vererbung an dieser Kostenstelle unterbrochen wird. Aktivieren Sie diese Option, um die Vererbung innerhalb der Kostenstellenhierarchie zu unterbrechen.
X500 Knoten	Aktivieren Sie diese Option, um die Kostenstelle für den Export in ein X500-Schema zu kennzeichnen.
Keine Vererbung an Personen	Gibt an, ob die Vererbung an Personen für die Kostenstelle vorübergehend verhindert werden soll.
Keine Vererbung an	Gibt an, ob die Vererbung an Geräte für die Kostenstelle

Eigenschaft	Beschreibung
Geräte	vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Gibt an, ob die Vererbung an Arbeitsplätze für die Kostenstelle vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Gibt an, ob für die Kostenstelle eine dynamische Rolle erstellt werden darf.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01 ... Freies Feld Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Rollentypen für Abteilungen, Kostenstellen und Standorte auf Seite 61
- Attestierer für Abteilungen, Kostenstellen und Standorte auf Seite 65
- Genehmiger und Genehmiger (IT) für Abteilungen, Kostenstellen und Standorte auf Seite 66
- Vererbung über Rollen blockieren auf Seite 32
- Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern auf Seite 33
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten auf Seite 91
- Zertifizierung von Abteilungen, Kostenstellen und Standorten auf Seite 96

Unternehmensbereich und Risikobewertung für Kostenstellen

Für die Risikobewertung einer Kostenstelle im Rahmen des Identity Audits können Sie hier Werte für die Einstufung der Kostenstelle erfassen.

Tabelle 16: Stammdaten zum Unternehmensbereich einer Kostenstelle

Eigenschaft	Beschreibung
Land	Land. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln.

Eigenschaft	Beschreibung
Bundesland	Bundesland. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln.
Unternehmensbereich	Unternehmensbereich der Kostenstelle. Die Angabe wird zur Risikobewertung der Kostenstelle benötigt.
Risikoindex (berechnet)	Für die Risikobewertung der Kostenstelle wird anhand der zugewiesenen Unternehmensressourcen ein Risikoindex berechnet. 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.*
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen an die Kostenstelle sind. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein. **0**: keine Transparenz **1**: volle Transparenz
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in dieser Kostenstelle zulässig sind. Der Wert kann bei der Prüfung von Complianceregeln ausgewertet werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln.* HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Complianceregeln vorhanden ist.
Umsatz des Bereichs	Umsatz der Kostenstelle.
Gewinn des Bereichs	Gewinn der Kostenstelle.

Verwandte Themen

- Ermitteln der Sprache für Personen auf Seite 161
- Ermitteln der Arbeitszeiten für Personen auf Seite 162
- Unternehmensbereiche für Abteilungen, Kostenstellen und Standorte auf Seite 63

Standorte erstellen und bearbeiten

Um einen Standort zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste einen Standort und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Standorte auf Seite 77
- Adressinformationen für Standorte auf Seite 80
- Netzwerkkonfiguration für Standorte auf Seite 81
- Anfahrtsbeschreibung für Standorte auf Seite 81
- Unternehmensbereich und Risikobewertung für Standorte auf Seite 81
- IT Betriebsdaten für Abteilungen, Kostenstellen und Standorte einrichten auf Seite 82

Allgemeine Stammdaten für Standorte

Für einen Standort erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 17: Allgemein Stammdaten eines Standortes

Eigenschaft	Beschreibung
Standort	Bezeichnung des Standorts. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Kurzname	Kurzbezeichnung des Standorts.
Bezeichnung	Zusätzliche Bezeichnung des Standorts.
Übergeordneter Standort	Übergeordneter Standort in der Rollenhierarchie. Um Standorte hierarchisch zu organisieren, wählen Sie in der Auswahlliste den übergeordneten Standort aus. Für einen Standort, der in der obersten Ebene einer Standorthierarchie steht, lassen Sie dieses Eingabefeld leer.

Eigenschaft	Beschreibung
Vollständiger Name	Kompletter Name des Standortes einschließlich übergeordneter Standorte. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Rollentyp	Rollentyp zur weiteren Klassifizierung.
Manager	Verantwortlicher Manager des Standorts.
2. Verantwortlicher	Stellvertretender Manager des Standorts.
Zusätzliche Manager	Anwendungsrolle für eine Gruppe von Managern und Stellvertretern, die diesen Standort verwalten. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge für den Standort zu entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Abteilung	Abteilung, dem der Standort primär zugeordnet ist.
Kostenstelle	Kostenstelle, der der Standort primär zugeordnet ist.
Zusatzbemerkung	Freitextfeld für zusätzliche Erläuterungen.
Genehmiger	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieses Standorts entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Genehmiger (IT)	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieses Standorts entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Zertifizierungsstatus	Zertifizierungsstatus des Standortes. Folgende

Eigenschaft	Beschreibung
	Zertifizierungsstatus können ausgewählt werden: • **Neu**: Der Standort wurde neu in der One Identity Manager-Datenbank angelegt. • **Zertifiziert**: Die Stammdaten des Standortes wurden durch einen Manager genehmigt. • **Abgelehnt**: Die Stammdaten des Standortes wurden durch einen Manager nicht genehmigt. Der Zertifizierungsstatus kann abhängig vom Ergebnis regelmäßiger Attestierungen gesetzt werden.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Deaktiviert	Gibt an, ob der Standort aktiv genutzt wird. Aktivieren Sie diese Option, wenn der Standort nicht genutzt wird. Die Option hat keinen Einfluss auf die Berechnung der Vererbung.
Vererbung blockieren	Gibt an, ob die Vererbung an diesem Standort unterbrochen wird. Aktivieren Sie diese Option, um die Vererbung innerhalb der Standorthierarchie zu unterbrechen.
X500 Knoten	Aktivieren Sie diese Option, um den Standort für den Export in ein X500-Schema zu kennzeichnen.
Keine Vererbung an Personen	Gibt an, ob die Vererbung an Personen für den Standort vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Gibt an, ob die Vererbung an Geräte für den Standort vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Gibt an, ob die Vererbung an Arbeitsplätze für den Standort vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Gibt an, ob für den Standort eine dynamische Rolle erstellt werden darf.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01 ... Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Rollentypen für Abteilungen, Kostenstellen und Standorte auf Seite 61
- Attestierer für Abteilungen, Kostenstellen und Standorte auf Seite 65
- Genehmiger und Genehmiger (IT) für Abteilungen, Kostenstellen und Standorte auf Seite 66
- Vererbung über Rollen blockieren auf Seite 32
- Vererbung an Personen, Geräte oder Arbeitsplätze für einzelne Rollen verhindern auf Seite 33
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten auf Seite 91
- Zertifizierung von Abteilungen, Kostenstellen und Standorten auf Seite 96

Adressinformationen für Standorte

Erfassen Sie die folgenden Stammdaten zur Erreichbarkeit des Standorts.

Tabelle 18: Adressdaten eines Standorts

Eigenschaft	Beschreibung
Adresse	Postanschrift des Standorts.
Straße	Straße.
Gebäude	Gebäude.
Postleitzahl	Postleitzahl.
Ort	Ort.
Land	Land. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln.
Bundesland	Bundesland. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln.
Telefon	Telefonnummer des Standorts.
Telefonkurzangabe	Telefonkurzwahl (ohne Vorwahl).
Fax	Faxnummer des Standorts.
Raum	Raum.
Bemerkung (Raum)	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Ermitteln der Sprache für Personen auf Seite 161
- Ermitteln der Arbeitszeiten für Personen auf Seite 162

Netzwerkkonfiguration für Standorte

Erfassen Sie Informationen über die Konfiguration des Netzwerkes am Standort.

Tabelle 19: Netzwerkinformationen eines Standorts

Eigenschaft	Beschreibung
IP-Offset	IP-Offset des Standorts.
Subnet-Maske	Subnet-Maske des Standorts.

Anfahrtsbeschreibung für Standorte

Erfassen Sie zusätzliche Besuchsadressen und eine eventuelle Anfahrtsbeschreibung zum Standort. Über die Schaltfläche neben dem Eingabefeld schalten Sie die Eingabe frei und können Einträge hinzufügen. Über die Schaltfläche können Sie Einträge aus der Auswahlliste entfernen.

Tabelle 20: Anfahrtsbeschreibung eines Standorts

Eigenschaft	Beschreibung
Besuchsadressen	Besuchsadressen des Standortes.
Fahrverbindungen	Fahrverbindungen zum Standort.

Unternehmensbereich und Risikobewertung für Standorte

Für die Risikobewertung eines Standorts im Rahmen des Identity Audits können Sie hier Werte für die Einstufung des Standortes erfassen.

Tabelle 21: Stammdaten zum Unternehmensbereich eines Standorts

Eigenschaft	Beschreibung
Unternehmensbereich	Unternehmensbereich des Standorts. Die Angabe wird zur

Eigenschaft	Beschreibung
	Risikobewertung des Standorts benötigt.
Risikoindex (berechnet)	Für die Risikobewertung des Standorts wird anhand der zugewiesenen Unternehmensressourcen ein Risikoindex berechnet. 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.*
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen an den Standort sind. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein. **0**: keine Transparenz **1**: volle Transparenz
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in diesem Standort zulässig sind. Der Wert kann bei der Prüfung von Complianceregeln ausgewertet werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln.* HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Complianceregeln vorhanden ist.
Umsatz des Bereichs	Umsatz des Standorts.
Gewinn des Bereichs	Gewinn des Standorts.

Verwandte Themen

- Unternehmensbereiche für Abteilungen, Kostenstellen und Standorte auf Seite 63

IT Betriebsdaten für Abteilungen, Kostenstellen und Standorte einrichten

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

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

Beispiel:

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

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager die Kategorie **Organisationen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste eine Rolle.
3. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
4. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.
   - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

     Um den Anwendungsbereich festzulegen

     a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.
     b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder, für eine Kontendefinition, die Tabelle `TSBAccountDef`.
     c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.
     d. Klicken Sie **OK**.
   - **Spalte**: Wählen Sie die Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.

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

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

5. Speichern Sie die Änderungen.

IT Betriebsdaten für Zielsysteme

Die IT Betriebsdaten, die in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen oder Ändern von Benutzerkonten und Postfächer für eine Person in den Zielsystemen verwendet werden, sind in der nachfolgenden Tabelle aufgeführt.

HINWEIS: Die IT Betriebsdaten sind abhängig vom Zielsystem und sind in den One Identity Manager Modulen enthalten. Die Daten stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 22: Zielsystemtyp-abhängige IT Betriebsdaten

Zielsystemtyp	IT Betriebsdaten
Active Directory	Container
	Homeserver
	Profilserver
	Terminal Homeserver
	Terminal Profilserver
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
Microsoft Exchange	Postfachdatenbank
LDAP	Container
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
Domino	Server
	Zertifikat
	Vorlage der Postdatei
	Identität
SharePoint	Authentifizierungsmodus
	Gruppen erbbar
	Rollen erbbar

Zielsystemtyp	IT Betriebsdaten
	Identität
	Privilegiertes Benutzerkonto
SharePoint Online	Gruppen erbbar
	Rollen erbbar
	Privilegiertes Benutzerkonto
	Authentifizierungsmodus
Kundendefinierte Zielsysteme	Container (je Zielsystem)
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
Azure Active Directory	Gruppen erbbar
	Administratorrollen erbbar
	Abonnements erbbar
	Unwirksame Dienstpläne erbbar
	Identität
	Privilegiertes Benutzerkonto
	Kennwort bei der nächsten Anmeldung ändern
Cloud Zielsystem	Container (je Zielsystem)
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
Unix-basierte Zielsysteme	Login-Shell
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
Oracle E-Business Suite	Identität
	Gruppen erbbar
	Privilegiertes Benutzerkonto
SAP R/3	Identität
	Gruppen erbbar
	Rollen erbbar
	Profile erbbar
	Strukturelle Profile erbbar

Zielsystemtyp	IT Betriebsdaten
	Privilegiertes Benutzerkonto
Exchange Online	Gruppen erbbar
Privileged Account Management	Authentifizierungsanbieter Gruppen erbbar Identität Privilegiertes Benutzerkonto
Google Workspace	Organisation Gruppen erbbar Produkte und SKUs erbbar Admin-Rollen-Zuordnungen erbbar Identität Privilegiertes Benutzerkonto Kennwort bei der nächsten Anmeldung ändern
OneLogin	Rollen erbbar Identität Privilegiertes Benutzerkonto Lizenzierungsstatus OneLogin Gruppe

IT Betriebsdaten ändern

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

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Personen, die Geräte und die Arbeitsplätze an die Abteilungen, Kostenstellen oder Standorte zu. Die Personen, die Geräte und die Arbeitsplätze können über diese Organisationen ihre Unternehmensressourcen erhalten.

Um Personen, Geräte und Arbeitsplätze in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Organisationen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die entsprechende Aufgabe.
   - **Personen zuweisen**
   - **Geräte zuweisen**

- **Arbeitsplätze zuweisen**

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Objekt und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

TIPP: Nutzen Sie dynamische Rollen, um Personen, Geräte und Arbeitsplätze automatisch an Abteilungen, Kostenstellen oder Standorte zuzuweisen.

Verwandte Themen

- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 25
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten auf Seite 91
- Personen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 150
- Geräte an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 184
- Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 192

Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen

Das Standardverfahren für die Zuweisung von Unternehmensressourcen an Personen, Geräte und Arbeitsplätze ist die indirekte Zuweisung. Dabei wird eine Person, ein Gerät oder ein Arbeitsplatz in Abteilungen, Kostenstellen oder Standorte eingeordnet. Aus der Position innerhalb der Hierarchie, der Vererbungsrichtung und den Unternehmensressourcen, die diesen Rollen zugeordnet sind, berechnet sich die Summe der zugeordneten Unternehmensressourcen für eine Person, ein Gerät oder einen Arbeitsplatz.

Die indirekte Zuweisung wird unterschieden in

- Sekundäre Zuweisung

  Die sekundäre Zuweisung erfolgt über die Einordnung einer Person, eines Gerätes oder eines Arbeitsplatzes in eine Rollenhierarchie. Die sekundäre Zuweisung ist das

Standardverfahren für die Zuweisung und Vererbung von Unternehmensressourcen über Rollen.

WICHTIG: Ob eine sekundäre Zuweisung von Unternehmensressourcen möglich ist, legen Sie an den Rollenklassen fest.

Erfüllt eine Person, ein Gerät oder ein Arbeitsplatz die Bedingungen einer dynamischen Rolle, so wird das Objekt dynamisch in die entsprechende Unternehmensstruktur aufgenommen und kann über diese Unternehmensressourcen erhalten.

- Primäre Zuweisung

  Die primäre Zuweisung erfolgt über die Fremdschlüssel-Referenzierung einer Abteilung, einer Kostenstelle oder eines Standortes in den Personen-, Geräte- und Arbeitsplatzobjekten. Die Vererbung über die primären Zuweisungen kann über Konfigurationsparameter aktiviert werden.

Damit Unternehmensressourcen an Personen, Geräte und Arbeitsplätze vererbt werden können, müssen Sie die Unternehmensressourcen an Abteilungen, Kostenstellen oder Standorte zuweisen. In der nachfolgenden Tabelle sind die möglichen Zuweisungen von Unternehmensressourcen dargestellt.

HINWEIS: Die Unternehmensressourcen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 23: Mögliche Zuweisungen von Unternehmensressourcen

Unternehmensressource	Verfügbar im Modul
Ressourcen	immer
Kontendefinitionen	Zielsystem Basismodul
Gruppen kundendefinierter Zielsysteme	Zielsystem Basismodul
Systemberechtigungen kundendefinierter Zielsysteme	Zielsystem Basismodul
Active Directory Gruppen	Active Directory Modul
SharePoint Gruppen	SharePoint Modul
SharePoint Rollen	SharePoint Modul
LDAP Gruppen	LDAP Modul
Notes Gruppen	Domino Modul
SAP Gruppen	SAP R/3 Benutzermanagement-Modul
SAP Profile	SAP R/3 Benutzermanagement-Modul
SAP Rollen	SAP R/3 Benutzermanagement-Modul
SAP Parameter	SAP R/3 Benutzermanagement-Modul
Strukturelle Profile	Modul SAP R/3 Strukturelle Profile Add-

Unternehmensressource	Verfügbar im Modul
	on
BI Analyseberechtigungen	Modul SAP R/3 Analyseberechtigungen Add-on
E-Business Suite Berechtigungen	Oracle E-Business Suite Modul
Systemrollen	Systemrollenmodul
Abonnierbare Berichte	Modul Berichtsabonnement
Software	Modul Softwaremanagement
Azure Active Directory Gruppen	Azure Active Directory Modul
Azure Active Directory Administratorrollen	Azure Active Directory Modul
Azure Active Directory Abonnements	Azure Active Directory Modul
Unwirksame Azure Active Directory Dienst-pläne	Azure Active Directory Modul
Unix Gruppen	Modul Unix-basierte Zielsysteme
Cloud Gruppen	Modul Cloud Systems Management
Cloud Systemberechtigungen	Modul Cloud Systems Management
PAM Benutzergruppen	Privileged Account Governance Modul
Google Workspace Gruppen	Google Workspace Modul
Google Workspace Produkte und SKUs	Google Workspace Modul
SharePoint Online Gruppen	SharePoint Online Modul
SharePoint Online Rollen	SharePoint Online Modul
OneLogin Rollen	OneLogin Modul

Um Unternehmensressourcen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Organisationen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe zum Zuweisen der entsprechenden Unternehmensressource.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Unternehmensressourcen zu.

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

   Um eine Zuweisung zu entfernen

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

Detaillierte Informationen zum Thema

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 25
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 26
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87
- Dynamische Rollen auf Seite 37

Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten

Über diese Aufgabe definieren Sie dynamische Rollen für einzelne Abteilungen, Kostenstellen oder Standorte. Damit können Sie Mitgliedschaften in diesen Rollen dynamisch festlegen.

HINWEIS: Die Aufgabe **Dynamische Rolle erstellen** wird nur für Abteilungen, Kostenstellen und Standorte angeboten, für welche die Option **Dynamische Rollen nicht erlaubt** nicht aktiviert ist.

Um eine dynamische Rolle zu erstellen

1. Wählen Sie im Manager die Kategorie **Organisationen > <Rollenklasse>.**
2. Wählen Sie in der Ergebnisliste eine Rolle.
3. Wählen Sie die Aufgabe **Dynamische Rolle erstellen**.
4. Erfassen Sie die erforderlichen Stammdaten.
5. Speichern Sie die Änderungen.

Um eine dynamische Rolle zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Organisationen > <Rollenklasse> > Dynamische Rollen**.
2. Wählen Sie in der Ergebnisliste eine Rolle.
3. Öffnen Sie das Überblicksformular der Rolle.

4. Wählen Sie das Formularelement **Dynamische Rollen** und klicken Sie auf die dynamische Rolle.
5. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
6. Bearbeiten Sie die Stammdaten der dynamische Rolle.
7. Speichern Sie die Änderungen.

Verwandte Themen

- Dynamische Rollen auf Seite 37
- Dynamische Rollen erstellen und bearbeiten auf Seite 38
- Allgemeine Stammdaten für Abteilungen auf Seite 68
- Allgemeine Stammdaten für Kostenstellen auf Seite 73
- Allgemeine Stammdaten für Standorte auf Seite 77

Dynamische Rollen mit fehlerhaft ausgeschlossenen Personen

Im Manager erhalten Sie einen Überblick über alle dynamischen Rollen mit widersprüchlichen Einträgen in der Ausschlussliste. Das heißt, für mindestens einen Eintrag in der Ausschlussliste gilt:

- Die Bedingung der dynamischen Rolle trifft nicht zu.

  Das kann beispielsweise auftreten, wenn die Bedingung der dynamischen Rolle geändert wurde, nachdem die Person in die Ausschlussliste eingetragen wurde.

  - ODER -

- Die ausgeschlossene Person ist auch über einen anderen Weg an die Rolle zugewiesen.

  Beispielsweise per Vererbung oder durch Direktzuweisung.

Prüfen Sie diese Einträge und korrigieren Sie die Zuweisungen.

Um widersprüchliche Einträge in der Ausschlussliste für Abteilungen, Standorte oder Kostenstellen zu prüfen

1. Wählen Sie im Manager die Kategorie **Organisationen > Fehlerdiagnose > Dynamische Rollen mit potentiell fehlerhaft ausgeschlossenen Personen**.
2. Wählen Sie in der Ergebnisliste die dynamische Rolle.
3. Wählen Sie die Aufgabe **Personen ausschließen**.

   In der Ausschlussliste sehen Sie, auf welche Personen die genannten Bedingungen zutreffen.

Verwandte Themen

- Stammdaten der Ausschlussliste für dynamische Rollen auf Seite 52
- Personen aus der Ausschlussliste entfernen auf Seite 52
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen und bearbeiten auf Seite 91

Organisationen zuweisen

Über diese Aufgabe können Sie Beziehungen einer Abteilung, Kostenstelle oder eines Standortes zu anderen Rollen abbilden. Die Aufgabe hat dieselbe Wirkung wie die Zuordnung von Abteilungen, Kostenstellen und Standorten auf den Stammdatenformularen der Rollen. Die Zuordnung wird in der jeweiligen Fremdschlüsselspalte der Basistabelle eingetragen.

Um eine Kostenstelle oder einen Standort an Abteilungen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Organisationen > Kostenstellen** oder **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Wählen Sie den Tabreiter **Abteilungen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abteilungen zu.

   Die ausgewählte Rolle wird allen Abteilungen als Kostenstelle beziehungsweise Standort primär zugewiesen.
6. Speichern Sie die Änderungen.

Um eine Abteilung oder einen Standort an Kostenstellen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen** oder **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Wählen Sie den Tabreiter **Kostenstellen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kostenstellen zu.

   Die ausgewählte Rolle wird allen Kostenstellen als Abteilung beziehungsweise Standort primär zugewiesen.
6. Speichern Sie die Änderungen.

Um eine Abteilung oder eine Kostenstelle an Standorte zuzuweisen

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen** oder **Organisationen > Kostenstellen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Wählen Sie den Tabreiter **Standorte**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Standorte zu.

   Die ausgewählte Rolle wird allen Standorten als Abteilung beziehungsweise Kostenstelle primär zugewiesen.
6. Speichern Sie die Änderungen.

Vererbungsausschluss für Abteilungen, Kostenstellen und Standorte festlegen

Um zu verhindern, dass Personen, Geräte oder Arbeitsplätze gleichzeitig an verschiedene Rollen zugewiesen werden und über diese Rollen sich ausschließende Unternehmensressourcen erhalten könnten, können Sie widersprechende Rollen definieren. Dabei legen Sie fest, welche Abteilungen, Kostenstellen oder Standorte sich gegenseitig ausschließen. Sie dürfen diese Rollen dann nicht mehr an ein und dieselbe Person (Gerät, Arbeitsplatz) zuweisen.

HINWEIS: Nur Rollen, die direkt als widersprechende Rollen definiert sind, können nicht an ein und dieselbe Person (Gerät, Arbeitsplatz) zugewiesen werden. Festlegungen an übergeordneten oder untergeordneten Rollen haben keinen Einfluss auf die Zuweisung.

Um den Vererbungsausschluss zu konfigurieren

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Structures | ExcludeStructures** und kompilieren Sie die Datenbank.

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

Um den Vererbungsausschluss für Abteilungen festzulegen

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen**.
2. Wählen Sie in der Ergebnisliste eine Abteilung.
3. Wählen Sie die Aufgabe **Widersprechende Abteilungen bearbeiten**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abteilungen zu, die sich mit der gewählten Abteilung ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Um den Vererbungsausschluss für Kostenstellen festzulegen

1. Wählen Sie im Manager die Kategorie **Organisationen > Kostenstellen**.
2. Wählen Sie in der Ergebnisliste eine Kostenstelle.
3. Wählen Sie die Aufgabe **Widersprechende Kostenstellen bearbeiten**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kostenstellen zu, die sich mit der gewählten Kostenstelle ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Kostenstellen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Um den Vererbungsausschluss für Standorte festzulegen

1. Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste einen Standort.
3. Wählen Sie die Aufgabe **Widersprechende Standorte bearbeiten**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Standorte zu, die sich mit dem gewählten Standort ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Standorte, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbungsausschluss: Festlegen widersprechender Rollen auf Seite 35

Zusatzeigenschaften an Abteilungen, Kostenstellen und Standorte zuweisen

An Abteilungen, Kostenstellen und Standorte können Sie Zusatzeigenschaften 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 festzulegen

1. Wählen Sie im Manager die Kategorie **Organisationen > <Rollenklasse>.**
2. Wählen Sie in der Ergebnisliste die Rolle.
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.

Verwandte Themen

- Zusatzeigenschaften einrichten auf Seite 220

Zertifizierung von Abteilungen, Kostenstellen und Standorten

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

Der Zertifizierungsstatus von Abteilungen, Kostenstellen und Standorten kann manuell oder durch regelmäßige Attestierungen gesetzt werden. Um den Zertifizierungsstatus durch Attestierungen zu setzen, konfigurieren Sie die Attestierungsrichtlinien entsprechend.

Um den Zertifizierungsstatus einer Abteilung, Kostenstelle oder eines Standorts manuell zu ändern

1. Bearbeiten Sie im Manager die Stammdaten der Abteilung, Kostenstelle oder des Standorts.
2. Wählen Sie im Eingabefeld **Zertifizierungsstatus** den gewünschten Wert.
3. Speichern Sie die Änderungen.

Um den Zertifizierungsstatus von Abteilungen, Kostenstellen oder Standorten durch Attestierungen zu ändern

1. Wählen Sie im Manager die Kategorie **Attestierung > Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie, durch deren Attestierungsläufe der Zertifizierungsstatus angepasst werden soll.
3. Wenn nach einer genehmigten Attestierung der Zertifizierungsstatus auf **Zertifziert** geändert werden soll, aktivieren Sie **Zertifizierungsstatus auf "Zertifiziert" setzen**.
4. Wenn nach einer abgelehnten Attestierung der Zertifizierungsstatus auf **Abgelehnt** geändert werden soll, aktivieren Sie **Zertifizierungsstatus auf "Abgelehnt" setzen**.
5. Speichern Sie die Änderungen.

Der One Identity Manager stellt Standardverfahren bereit, über welche die Stammdaten von Abteilungen, Kostenstellen und Standorten, die neu in die One Identity Manager-Datenbank aufgenommen wurden, zeitnah durch deren Manager attestiert und zertifiziert werden. Die Attestierung wird nur für Organisationen mit dem Zertifizierungsstatus **Neu** durchgeführt. Wenn die Attestierung genehmigt wird, wird der Zertifizierungsstatus der attestierten Organisation auf **Zertifiziert** gesetzt, andernfalls auf **Abgelehnt**. Wurde die Attestierung genehmigt, wird die Option **Keine Vererbung an Personen** deaktiviert.

HINWEIS: Wenn die Attestierung abgelehnt wurde, wird nur der Zertifizierungsstatus geändert. Weitere Verhaltensänderungen, beispielsweise in der Vererbungsberechnung, sind damit nicht verbunden und können unternehmensspezifisch implementiert werden.

Diese Funktion steht zur Verfügung, wenn das Zielsystem Basismodul vorhanden ist. Ausführliche Informationen zur Zertifizierung neuer Rollen und Organisationen finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Detaillierte Informationen zum Thema

- Abteilungen erstellen und bearbeiten auf Seite 67
- Kostenstellen erstellen und bearbeiten auf Seite 72
- Standorte erstellen und bearbeiten auf Seite 77

Berichte über Abteilungen, Kostenstellen und Standorte

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 Abteilungen, Kostenstellen und Standorte stehen folgende Berichte zur Verfügung.

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

Tabelle 24: Berichte über Abteilungen, Kostenstellen und Standorte

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Rollen, in denen die Personen der ausgewählten Abteilung, der ausgewählten Kostenstelle oder dem ausgewählten Standort ebenfalls Mitglied sind.
Datenqualität der Abteilungsmitglieder (Kostenstellenmitglieder)	Der Bericht wertet die Datenqualität der Personendatensätze aus. Berücksichtigt werden alle Personen der Abteilung oder der Kostenstelle.
Historische Mitgliedschaften anzeigen	Der Bericht listet alle Mitglieder der ausgewählten Abteilung, der ausgewählten Kostenstelle oder des ausgewählten Standortes und den Zeitraum ihrer Mitgliedschaft auf.
Personen pro Abteilung	Der Bericht enthält die Anzahl der Personen pro Abteilung. Berücksichtigt werden die primären und sekundären Zuweisungen der Personen zu den Organisationen. Den Bericht finden Sie im Manager in der Kategorie **Mein One Identity Manager**.
Personen pro Kostenstelle	Der Bericht enthält die Anzahl der Personen pro Kostenstelle. Berücksichtigt werden die primären und sekundären Zuweisungen der Personen zu den Organisationen. Den Bericht finden Sie im Manager in der Kategorie **Mein One Identity Manager**.
Personen pro Standort	Der Bericht enthält die Anzahl der Personen pro Standort. Berücksichtigt werden die primären und sekundären Zuweisungen der Personen zu den Organisationen. Den Bericht finden Sie im Manager in der Kategorie **Mein One Identity Manager**.

Verwandte Themen

- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 158

4

Personen verwalten

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Personen mit ihren Stammdaten und allen bereitgestellten Unternehmensressourcen. Als Unternehmensressourcen gelten dabei IT-Ressourcen, wie Geräte, Software und die Zugriffsberechtigungen in verschiedenen Zielsystemen. Daneben können auch Arbeitsmittel, wie Mobiltelefone, Dienstwagen oder Schlüssel, als Ressourcen an den Personen abgebildet werden.

Personen erhalten die Unternehmensressourcen entsprechend ihrer Funktion und ihrer Position innerhalb der Unternehmensstruktur. Unternehmensstrukturen, wie Abteilungen, Kostenstellen und Standorte, werden ebenfalls im One Identity Manager abgebildet. Ebenso die Mitgliedschaft der Personen in diesen Unternehmensstrukturen. Sobald Unternehmensressourcen an die Unternehmensstrukturen zugewiesen werden, werden diese Unternehmensressourcen an alle Mitglieder vererbt. Personen können so automatisiert mit allen benötigten Unternehmensressourcen versorgt werden.

Wenn Sie die Zugriffsberechtigungen auf die One Identity Manager-Werkzeuge über Anwendungsrollen verwalten, erhalten Sie alle Informationen über die aktuellen Zugriffsberechtigungen und Verantwortlichkeiten der Personen innerhalb des One Identity Manager.

Die One Identity Manager Bestandteile für die Verwaltung von Personen sind verfügbar, wenn der Konfigurationsparameter **QER | Person** aktiviert ist.

- Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter.

Detaillierte Informationen zum Thema

- Zentrales Benutzerkonto einer Person auf Seite 107
- Standard-E-Mail-Adresse einer Person auf Seite 108
- Zentrales Kennwort einer Person auf Seite 108
- Abbildung mehrerer Identitäten einer Person auf Seite 110
- Kennwortrichtlinien für Personen auf Seite 113
- Personen erstellen und bearbeiten auf Seite 127
- Deaktivieren und Löschen von Personen auf Seite 138
- Löschen aller personenbezogenen Daten auf Seite 141

- Eingeschränkter Zugang zum One Identity Manager auf Seite 142
- Unternehmensressourcen an Personen zuweisen auf Seite 144
- Herkunft von Rollen und Berechtigungen von Personen anzeigen auf Seite 156
- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 158
- Berichte über Personen auf Seite 164
- Konfigurationsparameter für die Verwaltung von Personen auf Seite 230

One Identity Manager Benutzer für die Personenverwaltung

In die Verwaltung von Personen sind folgende Benutzer eingebunden.

Tabelle 25: Benutzer

Benutzer	Aufgaben
Administratoren für Personen	Personenadministratoren müssen der Anwendungsrolle **Identity Management | Personen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Stammdaten aller Personen. • Ordnen den Personen Manager zu. • Weisen Unternehmensressourcen an die Personen zu. • Überprüfen und autorisieren die Stammdaten von Personen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Bearbeiten Kennwortrichtlinien für Kennwörter von Personen. • Können Sicherheitsschlüssel (Webauthn) von Personen löschen. • Können im Web Portal die Bestellungen, Attestierungen und Delegierungen aller Personen sehen und Delegierungen bearbeiten.
Personenverantwortliche	Die Anwendungsrolle **Basisrollen | Personenverantwortliche** wird einem Benutzer automatisch zugewiesen, wenn der Benutzer Manager oder Verantwortlicher von Personen, Abteilungen, Standorten, Kostenstellen, Geschäftsrollen oder IT Shops ist.

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Stammdaten der Objekte, für die sie verantwortlich sind, und weisen ihnen Unternehmensressourcen zu. • Können im Web Portal neue Personen anlegen und die Stammdaten ihrer Mitarbeiter bearbeiten. • Können ihre Mitarbeiter in den IT Shop aufnehmen. • Können im Web Portal die Complianceregelverletzungen ihrer Mitarbeiter sehen. • Können im Web Portal Delegierungen für ihre Mitarbeiter erstellen. • Können im Web Portal die Delegierungen ihrer Mitarbeiter sehen und bearbeiten. Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Basisdaten für Personenstammdaten

Für die Personenverwaltung werden die folgenden Basisdaten benötigt.

- 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**.

- Partnerfirmen

  Bei der Erfassung externer Personen muss eine Firma angegeben werden.

- Mailvorlagen

  Die Anmeldeinformationen für neue Benutzerkonten in einem Zielsystem 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.

- Kennwortrichtlinien

  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`).

Detaillierte Informationen zum Thema

- Partnerfirmen für externe Personen erstellen und bearbeiten auf Seite 102
- Mailvorlagen für Benachrichtigungen über Personen auf Seite 104
- Kennwortrichtlinien für Personen auf Seite 113
- Konfigurationsparameter für die Verwaltung von Personen auf Seite 230

Partnerfirmen für externe Personen erstellen und bearbeiten

Um externe Personen zu verwalten, benötigen Sie die Angaben zu den Partnerfirmen. Erfassen Sie die Angaben zu externen Firmen.

Um eine Partnerfirma zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Partnerfirmen**.

2. Wählen Sie in der Ergebnisliste eine Firma und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Erfassen Sie die folgenden Stammdaten für eine Firma.

Tabelle 26: Allgemeine Stammdaten einer Firma

Eigenschaft	Beschreibung
Firma	Kurzbezeichnung der Firma für die Anzeige in den One Identity Manager-Werkzeugen.
Bezeichnung	Vollständige Bezeichnung der Firma.
Namenszusatz	Ergänzung zur Bezeichnung der Firma.
Kurzname	Kurzname der Firma.
Kontakt	Ansprechpartner der Firma.
Partner	Gibt an, ob es sich um eine Partnerfirma handelt.
Kundennummer	Kundennummer bei der Partnerfirma.
Lieferant	Gibt an, ob es sich um einen Lieferanten handelt.
Kundennummer	Kundennummer beim Lieferanten.
Leasing-Partner	Gibt an, ob es sich um einen Leasinggeber oder Vermieter handelt.
Hersteller	Gibt an, ob es sich um eine Herstellerfirma handelt.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.

Tabelle 27: Adressdaten einer Firma

Eigenschaft	Beschreibung
Straße	Straße.
Gebäude	Gebäude.
Postleitzahl	Postleitzahl.
Ort	Ort.
Bundesland	Bundesland.
Land	Land.
Telefon	Telefonnummer der Firma.

Eigenschaft	Beschreibung
Fax	Faxnummer der Firma.
E-Mail-Adresse	E-Mail-Adresse der Firma.
Webseite	Webseite der Firma. Über die Schaltfläche wird die angegebene Webseite im Standardwebbrowser angezeigt.

Mailvorlagen für Benachrichtigungen über Personen

Der One Identity Manager stellt standardmäßig Mailvorlagen bereit. Diese Mailvorlagen werden in den Sprachen Deutsch und Englisch bereitgestellt. Wenn Sie den Mailtext in anderen Sprachen benötigen, können Sie Maildefinitionen für diese Sprachen zu den Standard-Mailvorlagen hinzufügen.

Um Standard-Mailvorlagen zu bearbeiten

- Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen > Vordefiniert**.

Verwandte Themen

- Maildefinitionen für Personen erstellen und bearbeiten auf Seite 104
- Basisobjekte für Mailvorlagen über Personen auf Seite 105
- Mailvorlagen für Personen bearbeiten auf Seite 106

Maildefinitionen für Personen erstellen und bearbeiten

Ausführliche Informationen zum Erstellen und Bearbeiten von Mailvorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

In einer Mailvorlage können die Mailtexte in den verschiedenen Sprachen definiert werden. Somit wird bei Generierung einer E-Mail-Benachrichtigung die Sprache des Empfängers berücksichtigt.

Um eine neue Maildefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen**.

2. Wählen Sie in der Ergebnisliste eine Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie in der Auswahlliste **Sprachkultur** die Sprache, für welche die Maildefinition gelten soll.

   Angezeigt werden alle Sprachen, die aktiviert sind. Um weitere Sprachen zu verwenden, aktivieren Sie im Designer die entsprechenden Länder. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
4. Erfassen Sie im Eingabefeld **Betreff** die Betreffzeile.
5. Bearbeiten Sie in der Ansicht **Maildefinition** den Mailbody mit Hilfe des Mailtexteditors.
6. Speichern Sie die Änderungen.

Um eine vorhandene Maildefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen**.
1. Wählen Sie in der Ergebnisliste eine Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
2. In der Auswahlliste **Maildefinition** wählen Sie die Sprache für die Maildefinition.

   HINWEIS: Wenn der **Common | MailNotification | DefaultCulture** aktiviert ist, wird beim Öffnen einer Mailvorlage die Maildefinition in der Standardsprache für E-Mail-Benachrichtigungen geladen und angezeigt.
3. Bearbeiten Sie die Betreffzeile und den Mailbody.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Basisobjekte für Mailvorlagen über Personen auf Seite 105

Basisobjekte für Mailvorlagen über Personen

Die Angabe eines Basisobjekts in einer Mailvorlage ist nur erforderlich, wenn in der Maildefinition Eigenschaften des Basisobjekts referenziert werden.

In der Betreffzeile und im Mailbody einer Maildefinition können Sie alle Eigenschaften des unter **Basisobjekt** eingetragenen Objektes verwenden. Zusätzlich können Sie die Eigenschaften der Objekte verwenden, die per Fremdschlüsselbeziehung referenziert werden.

Zum Zugriff auf die Eigenschaften nutzen Sie die $-Notation. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verwandte Themen

- Maildefinitionen für Personen erstellen und bearbeiten auf Seite 104
- Mailvorlagen für Personen bearbeiten auf Seite 106

Mailvorlagen für Personen bearbeiten

Ausführliche Informationen zum Erstellen und Bearbeiten von Mailvorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Eine Mailvorlage besteht aus allgemeinen Stammdaten wie beispielsweise Zielformat, Wichtigkeit oder Vertraulichkeit der E-Mail Benachrichtigung sowie einer oder mehreren Maildefinitionen. Über die Maildefinitionen werden die Mailtexte in den verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail-Benachrichtigung die Sprache des Empfängers berücksichtigt.

Um Mailvorlagen zu erstellen und zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen**.
2. Wählen Sie in der Ergebnisliste eine Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .

   Der Mailvorlageneditor wird geöffnet.
3. Bearbeiten Sie die Mailvorlage.
4. Speichern Sie die Änderungen.

Um eine Mailvorlage zu kopieren

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen**.
2. Wählen Sie in der Ergebnisliste die Mailvorlage, die Sie kopieren möchten, und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Mailvorlage kopieren**.
4. Erfassen Sie im Eingabefeld **Name der Kopie** den Namen der neuen Mailvorlage.
5. Klicken Sie **OK**.

Um die Vorschau einer Mailvorlage anzuzeigen

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen**.

2. Wählen Sie in der Ergebnisliste die Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Vorschau**.
4. Wählen Sie das Basisobjekt.
5. Klicken Sie **OK**.

Um eine Mailvorlage zu löschen

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Mailvorlagen**.
2. Wählen Sie in der Ergebnisliste die Mailvorlage.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Maildefinitionen für Personen erstellen und bearbeiten auf Seite 104

Zentrales Benutzerkonto einer Person

Tabelle 28: Konfigurationsparameter für die Bildung der zentralen Benutzerkonten

Konfigurationsparameter	Bedeutung
QER | Person | CentralAccountGlobalUnique	Legt fest, wie das zentrale Benutzerkonto abgebildet wird. Ist der Konfigurationsparameter aktiviert, erfolgt die Bildung des zentralen Benutzerkonto einer Person eindeutig bezogen auf die zentralen Benutzerkonten aller Personen und die Benutzerkontennamen aller erlaubten Zielsysteme. Ist der Konfigurationsparameter nicht aktiviert, erfolgt die Bildung nur eindeutig bezogen auf die zentralen Benutzerkonten aller Personen.

Das zentrale Benutzerkonto einer Person wird zur Bildung des Anmeldenamens der Benutzerkonten in den aktivierten Zielsystemen herangezogen. Das zentrale Benutzerkonto wird weiterhin bei der Anmeldung an den Werkzeugen des One Identity Manager genutzt. In der Standardinstallation des One Identity Manager wird das zentrale Benutzerkonto aus dem Vornamen und dem Nachnamen der Person gebildet. Ist nur eine dieser Eigenschaften bekannt, wird diese zur Bildung des zentralen Benutzerkontos genutzt. Der One Identity Manager prüft in jedem Fall, ob es bereits ein zentrales

Benutzerkonto mit dem ermittelten Wert gibt. Ist dies der Fall, wird eine fortlaufende Nummerierung, beginnend mit 1, an den ursprünglichen Wert angehängt.

Tabelle 29: Beispiel für die Bildung des zentralen Benutzerkontos

Vorname	Nachname	Zentrales Benutzerkonto
Clara		CLARA
	Harris	HARRIS
Clara	Harris	CLARAH
Clara	Harrison	CLARAH1

Standard-E-Mail-Adresse einer Person

Die Standard-E-Mail-Adresse der Person wird auf die Postfächer in den aktivierten Zielsystemen abgebildet. In der Standardinstallation des One Identity Manager wird die Standard-E-Mail-Adresse aus dem zentralen Benutzerkonto der Person und der Standardmaildomäne der aktivierten Zielsysteme gebildet.

Die Standardmaildomäne wird aus dem Konfigurationsparameter **QER | Person | DefaultMailDomain** ermittelt.

- Aktivieren Sie im Designer den Konfigurationsparameter und tragen Sie die Bezeichnung der Standardmaildomäne als Wert ein.

Verwandte Themen

- Zentrales Benutzerkonto einer Person auf Seite 107

Zentrales Kennwort einer Person

Das zentrale Kennwort einer Person kann für die Anmeldung an den Zielsystemen und für die Anmeldung am One Identity Manager verwendet werden. Abhängig von der Konfiguration wird dazu das zentrale Kennwort einer Person an ihre Benutzerkonten und auf ihr Systembenutzerkennwort publiziert.

- Um die Änderung des zentralen Kennwortes einer Person in alle bestehenden Benutzerkonten der Person zu publizieren, prüfen Sie im Designer, ob der Konfigurationsparameter **QER | Person | UseCentralPassword** aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter.
- Um das zentrale Kennwort einer Person auf ihr Systembenutzerkennwort zur Anmeldung zu übernehmen, prüfen Sie im Designer, ob der Konfigurationsparameter

QER | Person | UseCentralPassword | SyncToSystemPassword aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter.

- Soll ein gesperrtes Systembenutzerkonto einer Person bei der Eingabe des zentralen Kennwortes entsperrt werden, prüfen Sie im Designer, ob der Konfigurationsparameter **QER | Person | UseCentralPassword | SyncToSystemPassword | UnlockByCentralPassword** aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter.

HINWEIS:

- Auf das zentrale Kennwort einer Person wird die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** angewendet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die zielsystemspezifischen Kennwortrichtlinien verstößt.
- Über den Konfigurationsparameter **QER | Person | UseCentralPassword | CheckAllPolicies** kann festgelegt werden, ob das zentrale Kennwort einer Person gegen alle Kennwortrichtlinien der Zielsysteme geprüft werden soll, in denen die Person Benutzerkonten besitzt. Die Prüfung erfolgt nur im Kennwortrücksetzungsportal.
- Das zentrale Kennwort einer Person wird nur dann an ein Benutzerkonto publiziert, wenn das Zielsystem des Benutzerkontos durch den One Identity Manager synchronisiert wird.
- Wird ein Zielsystem nur gelesen, wird das zentrale Kennwort einer Person nicht auf Benutzerkonten in diesem Zielsystem übertragen.
- Das zentrale Kennwort einer Person wird nicht auf privilegierte Benutzerkonten der Person publiziert.
- Kann ein Kennwort aufgrund eines Fehlers nicht geändert werden, erhält die Person eine entsprechende E-Mail Benachrichtigung.
- Um das zentrale Kennwort einer Person in eine Kennwortspalte einer kundenspezifischen Benutzerkontentabelle zu publizieren, definieren Sie im Designer ein ViewAddOn für die Sicht `QERVPersonCentralPwdColumn`. Die Datenbanksicht liefert die Kennwortspalte der Benutzerkontentabellen. Die Benutzerkontentabelle muss einen Verweis auf die Person haben (`UID_Person`) sowie eine Spalte `XMarkedForDeletion`. Ausführliche Informationen zum Anpassen des One Identity Manager Schemas finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Sollen weitere kundenspezifische Besonderheiten abgebildet werden, überschreiben Sie das Skript `QER_Publish_CentralPassword`. Ausführliche Informationen zum Bearbeiten von Skripten finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Das zentrale Kennwort, das Systembenutzerkennwort und die Kennwörter der Benutzerkonten können über das Kennwortrücksetzungsportal geändert werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch* und im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Verwandte Themen

- Sonstige Personenstammdaten auf Seite 134
- Kennwortrichtlinien für Personen auf Seite 113
- Gesperrte Personen und Systembenutzer anzeigen auf Seite 126

Abbildung mehrerer Identitäten einer Person

Tabelle 30: Konfigurationsparameter für die Abbildung mehrerer Identitäten

Konfigurationsparameter	Wirkung bei Aktivierung
Person | MasterIdentity | UseMasterForAuthentication	Legt fest, ob zur Anmeldung an One Identity Manager-Werkzeugen über Personen-basierte Authentifizierungsmodule die Hauptidentität genutzt werden soll. Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität für personengebundene Authentifizierungen genutzt. Ist der Konfigurationsparameter deaktiviert, wird die Subidentität für personengebundene Authentifizierungen genutzt. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen und zum Bearbeiten von Systembenutzern finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

In großen Unternehmen hat eine Person unter Umständen für ihre Arbeit unterschiedliche Identitäten, die beispielsweise aus unterschiedlichen Verträgen für unterschiedliche Tochterunternehmen resultieren. Diese Identitäten können sich beispielsweise in der Zugehörigkeit zu Abteilungen oder Kostenstellen oder in den Zugriffsberechtigungen unterscheiden. Ebenso können externe Mitarbeiter an unterschiedlichen Standorten eingesetzt werden und mit verschiedenen Identitäten im System abgebildet sein. Um die einzelnen Identitäten einer Person abzubilden und an einer zentralen Stelle zusammenzuführen, können Sie im One Identity Manager Hauptidentitäten und Subidentitäten für eine Person definieren.

In Zielsystemen werden unterschiedliche Typen von Benutzerkonten bereitgestellt, um die Personen mit unterschiedlichen Berechtigungen zu versorgen. Eine Person kann mit unterschiedlichen Identitäten mehrere Benutzerkonten mit unterschiedlichen Typen nutzen. Um die Zuweisung von Berechtigungen in den Zielsystemen besser steuern zu können, werden die Subidentitäten der Personen in verschiedene Identitätstypen unterteilt. Diese Einteilung entspricht den Benutzerkontentypen.

Hauptidentität

- Eine Hauptidentität repräsentiert eine wirkliche Person.
- Einer Hauptidentität können im One Identity Manager Benutzerkonten und Berechtigungen zugewiesen werden und sie kann innerhalb des IT Shops Bestellungen auslösen.
- Für eine Hauptidentität werden im One Identity Manager Personenstammdaten abgebildet.
- Eine Hauptidentität kann mehrere Subidentitäten besitzen.

Subidentität

- Eine Subidentität ist eine virtuelle Person.
- Einer Subidentität können im One Identity Manager Benutzerkonten und Berechtigungen zugewiesen werden und sie kann innerhalb des IT Shops Bestellungen auslösen.
- Eine Subidentität ist immer einer Hauptidentität zugeordnet.
- Für eine Subidentität werden im One Identity Manager die Personenstammdaten abgebildet. Diese können über entsprechend definierte Bildungsregeln aus den Personenstammdaten der Hauptidentität übernommen werden.
- Für eine Subidentität geben Sie auf dem Stammdatenformular der Person über die Auswahlliste **Hauptidentität** die Hauptidentität an.

TIPP: Wenn eine Person mit mehreren Identitäten arbeitet, aber bisher nur eine Identität davon im One Identity Manager bekannt war, dann sollten Sie

- eine Hauptidentität für die Person erstellen
- die bisher bekannte Identität als Subidentität zuordnen
- für die weiteren Identitäten neue Subidentitäten erstellen

Auf diese Weise ist beispielsweise innerhalb eines Identity Audits die Überprüfung der zulässigen Berechtigungen der Person pro Subidentität oder für die Hauptidentität, unter Einbeziehung aller Subidentitäten, möglich.

Verwandte Themen

- Identitätstypen von Personen auf Seite 111

Identitätstypen von Personen

Um die verschiedenen Identitäten einer Person zu differenzieren, nutzen Sie die folgenden Identitätstypen.

Tabelle 31: Identitätstypen

Wert	Beschreibung
Primäre Identität	Standardidentität für eine Person. Die Person besitzt ein Standardbenutzerkonto.
Organisatorische Identität	Virtuelle Person (Subidentität), zur Abbildung unterschiedlicher Rollen einer Person in der Organisation. Die Subidentität besitzt ein Benutzerkonto vom Typ **Organisatorische Identität**. Erfassen Sie zusätzlich eine Hauptidentität.
Persönliche Administratoridentität	Virtuelle Person (Subidentität), die ein Benutzerkonto vom Typ **Persönliche Administratoridentität** besitzt. Erfassen Sie zusätzlich eine Hauptidentität.
Zusatzidentität	Pseudo-Person, die mit einem Benutzerkonto vom Typ **Zusatzidentität** verbunden ist. Weisen Sie der Person einen Manager zu.
Gruppenidentität	Pseudo-Person, die mit einem administrativen Benutzerkonto vom Typ **Gruppenidentität** verbunden ist. Weisen Sie der Person einen Manager zu.
Dienstidentität	Pseudo-Person, die mit einem Benutzerkonto vom Typ **Dienstidentität** verbunden ist. Weisen Sie der Person einen Manager zu.
Maschinenidentität	Pseudo-Person zur Abbildung von Maschinenidentitäten.

Die primäre Identität, die organisatorische Identität und die persönliche Administratoridentität sind verschiedene Identitäten, unter denen ein und dieselbe Person ihre unterschiedlichen Aufgaben im Unternehmen ausführen kann.

Personen mit einer persönlichen Administratoridentität oder einer organisatorische Identität richten Sie als Subidentitäten ein. Diese Subidentitäten verbinden Sie mit den Benutzerkonten. Somit können für die unterschiedlichen Benutzerkonten die erforderlichen Berechtigungen erteilt werden.

Die Zusatzidentität, die Gruppenidentität und die Dienstidentität stellen Pseudo-Personen dar, über welche die verbundenen Benutzerkonten mit den Berechtigungen in den jeweiligen Zielsystemen versorgt werden. Durch die Einordnung der Pseudo-Personen in hierarchische Rollen oder als Kunden im IT Shop können Berechtigungen an die Benutzerkonten zugewiesen werden. Bestellungen im IT Shop kann nur der Manager dieser Pseudo-Personen auslösen. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob Pseudo-Personen gesondert betrachtet werden müssen.

Verwandte Themen

- Sonstige Personenstammdaten auf Seite 134
- Abbildung mehrerer Identitäten einer Person auf Seite 110

Kennwortrichtlinien für Personen

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 113
- Kennwortrichtlinien für Personen anwenden auf Seite 114
- Kennwortrichtlinien für Personen erstellen auf Seite 117
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 121
- Ausschlussliste für Kennwörter festlegen auf Seite 124
- Kennwörter für Personen prüfen auf Seite 125
- Generieren von Kennwörtern für Personen testen auf Seite 125
- Personen über ablaufende Kennwörter informieren auf Seite 126

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

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

Kennwortrichtlinien für Benutzerkonten

Es werden vordefinierte Kennwortrichtlinien bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können. Kennwortrichtlinien für Benutzerkonten können Sie für verschiedene Basisobjekte definieren, beispielsweise für Kontendefinitionen, Automatisierungsgrade oder für Zielsysteme.

Ausführliche Informationen zu Kennwortrichtlinien für Benutzerkonten finden Sie in den Administrationshandbüchern der Zielsysteme.

Verwandte Themen

- Zentrales Kennwort einer Person auf Seite 108

Kennwortrichtlinien für Personen anwenden

Für die Kennwörter von Personen sind Kennwortrichtlinien **One Identity Manager Kennwortrichtlinie** und **Kennwortrichtlinie für zentrales Kennwort von Personen** vordefiniert.

Sie können den Kennwortspalten der Personen kundenspezifische Kennwortrichtlinien zuweisen. Des Weiteren können Sie die Kennwortrichtlinien an Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zuweisen und somit Kennwortrichtlinien abhängig von der organisatorischen Einordnung der Personen anwenden.

Die anzuwendende Kennwortrichtlinie für eine Person wird in folgender Reihenfolge ermittelt:

1. Kennwortrichtlinie der primären Geschäftsrolle der Person
2. Kennwortrichtlinie der primären Abteilung der Person

3. Kennwortrichtlinie der primären Standort der Person
4. Kennwortrichtlinie der primären Kostenstelle der Person
5. Allgemeine Kennwortrichtlinie für Personenkennwörter
6. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie)

Verwandte Themen

- Vordefinierte Kennwortrichtlinien auf Seite 113
- Kennwortrichtlinien für Kennwortspalten ändern auf Seite 115
- Kennwortrichtlinien an Abteilungen, Kostenstellen, Standorte und Geschäftsrollen zuweisen auf Seite 115

Kennwortrichtlinien für Kennwortspalten ändern

Wenn Sie auf die Kennwortspalten von Personen nicht die vordefinierten Kennwortrichtlinien anwenden möchten, ändern Sie im Manager die Zuweisung der Kennwortrichtlinie zum Basisobjekt.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

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

Kennwortrichtlinien an Abteilungen, Kostenstellen, Standorte und Geschäftsrollen zuweisen

Die Kennwortrichtlinien für die Bildung des Systembenutzerkennworts einer Person, des Zugangscodes und des zentralen Kennwortes einer Person können Sie an Abteilungen, Kostenstellen, Standorte und Geschäftsrollen zuweisen.

HINWEIS: Wenn Sie die Zuweisung einer Kennwortrichtlinie über Unternehmensstrukturen nutzen möchten, sollten Sie sich entscheiden, ob Sie dafür Abteilungen oder Kostenstellen oder Standorte oder Geschäftsrollen verwenden. Anderenfalls könnten Performanceprobleme bei der Ermittlung der gültigen Kennwortrichtlinie auftreten. Eine große Anzahl von Hierarchie-Ebenen könnte ebenfalls zu Performanceproblemen bei der Ermittlung der anzuwendenden Kennwortrichtlinie führen.

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Basisdaten zur Konfiguration > Kennwortrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.
    - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

      Um den Anwendungsbereich festzulegen

      1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.
      2. Wählen Sie unter **Tabelle** die Tabelle, die die Basisobjekte enthält. Zur Auswahl stehen:
          - Abteilungen (Tabelle `Department`)
          - Geschäftsrollen (Tabelle `Org`)

            HINWEIS: Diese Tabelle ist verfügbar, wenn das Geschäftsrollenmodul vorhanden ist.
          - Standorte (Tabelle `Locality`)
          - Kostenstellen (Tabelle `Profitcenter`)
      3. Wählen Sie unter **Anwenden auf** die konkrete Abteilung, Kostenstelle, den Standort oder die Geschäftsrolle.
      4. Klicken Sie **OK**.
    - **Kennwortspalte**: Bezeichnung der Kennwortspalte. Zur Auswahl stehen:
        - **Personen -Zentrales Kennwort** (Tabelle `Person`, Spalte `CentralPassword`)
        - **Personen - Kennwort** (Tabelle `Person`, Spalte `DialogUserPassword`)
        - **Personen - Zugangscode** (Tabelle `Person`, Spalte `Passcode`)
    - **Kennwortrichtlinie**: Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.
5. Speichern Sie die Änderungen.

Kennwortrichtlinien für Personen bearbeiten

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

Um eine Kennwortrichtlinie zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 118
- Richtlinieneinstellungen für Kennwortrichtlinien auf Seite 118
- Zeichenklassen für Kennwörter auf Seite 120
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 121

Kennwortrichtlinien für Personen erstellen

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

Um eine Kennwortrichtlinie zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 118
- Richtlinieneinstellungen für Kennwortrichtlinien auf Seite 118
- Zeichenklassen für Kennwörter auf Seite 120
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 121

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 32: Stammdaten einer Kennwortrichtlinie

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

Richtlinieneinstellungen für Kennwortrichtlinien

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

Tabelle 33: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, dann wird das initiale Kennwort benutzt. HINWEIS: Das initiale Kennwort wird nicht für das System-

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

Eigenschaft	Bedeutung
Namensbestandteile unzulässig	Gibt an, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

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

Tabelle 34: Zeichenklassen für Kennwörter

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

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

Kundenspezifische Skripte für Kennwortanforderungen

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

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 122
- Skript zum Generieren eines Kennwortes auf Seite 123

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Kennwort, das zu prüfen ist

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

Beispiel: Skript zum Prüfen eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Personen > 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 123

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Generiertes Kennwort

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

Beispiel: Skript zum Generieren eines Kennwortes

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

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

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

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Personen > 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 122

Ausschlussliste für Kennwörter festlegen

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

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

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

Kennwörter für Personen prüfen

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

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

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

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

Generieren von Kennwörtern für Personen 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 **Personen > 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.

Personen über ablaufende Kennwörter informieren

Um einen Benutzer darüber zu informieren, dass sein Kennwort abläuft, werden verschiedene Funktionen eingesetzt:

- Bei der Anmeldung am One Identity Manager wird der Benutzer auf ein ablaufendes Kennwort hingewiesen und kann sein Kennwort gegebenenfalls ändern.
- Das System verschickt für Personen-basierte Authentifizierungsmodule Erinnerungsbenachrichtigungen zu ablaufenden Kennwörtern ab 7 Tage vor dem Ablauf des Kennwortes.
    - Die Zeit in Tagen können Sie im Konfigurationsparameter **Common | Authentication | DialogUserPasswordReminder** anpassen. Bearbeiten Sie den Konfigurationsparameter im Designer.
    - Die Benachrichtigungen werden nach dem Zeitplan **Erinnerung Ablauf des Systembenutzerkennwortes** ausgelöst und verwenden die Mailvorlage **Person-Systembenutzerkennwort läuft ab**. Den Zeitplan und die Mailvorlage können Sie bei Bedarf im Designer anpassen.

Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen und zum Bearbeiten von Systembenutzern finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Gesperrte Personen und Systembenutzer anzeigen

Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden.

- Gesperrte Personen werden im Manager in der Kategorie **Personen > Gesperrte Personen** angezeigt. Auf dem Überblicksformular einer Person wird ein zusätzlicher Hinweis zur gesperrten Anmeldung angezeigt.
- Gesperrte Systembenutzer werden im Designer in der Kategorie **Berechtigungen > Systembenutzer > Gesperrte Systembenutzer** angezeigt. Auf dem Überblicksformular eines Systembenutzers wird ein zusätzlicher Hinweis zur gesperrten Anmeldung angezeigt.

Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Damit werden die Personen und Systembenutzer wieder entsperrt. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch* und im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Verwandte Themen

- Zentrales Kennwort einer Person auf Seite 108

Personen erstellen und bearbeiten

Im One Identity Manager können Sie die Stammdaten zu Personen eines Unternehmens sowie zu externen Personen verwalten. Da sich die abgebildeten Stammdaten für interne und externe Personen nicht unterscheiden, wird in der weiteren Beschreibung der Begriff **Person** verwendet.

Die Personenstammdaten erfassen Sie im Manager in der Kategorie **Personen**. In dieser Kategorie werden die Personen nach unterschiedlichen Kriterien gefiltert.

- **Personen**: Alle aktivierten und zeitweilig deaktivierten Personen.
- **Inaktive Personen**: Alle dauerhaft deaktivierten Personen.
- **Gesperrte Personen**: Alle Person die aufgrund falscher Kennworteingabe gesperrt sind.
- **Zertifizierung**: Alle Personen nach ihrem Zertifizierungsstatus.
- **Datenquelle**: Alle Personen nach ihrer Importdatenquelle.
- **Identität**: Alle Personen nach ihrem Identitätstyp.

Um Personen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste eine Person aus und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   – ODER –

   Klicken Sie in der Ergebnisliste .

   Das Stammdatenformular für eine Person wird geöffnet.
3. Bearbeiten Sie die Stammdaten der Person.
4. Speichern Sie die Änderungen.

Achten Sie beim Bearbeiten der Personenstammdaten darauf, dass Sie alle Pflichtfelder ausfüllen. Einige der Stammdaten werden über Bildungsregeln an die Benutzerkonten einer Person vererbt.

HINWEIS: Eigenschaften von Personen, die aus einem angeschlossenen Zielsystem eingelesen wurden, können im One Identity Manager nur eingeschränkt bearbeitet werden. Bestimmte Eigenschaften sind für die Bearbeitung gesperrt, da hierfür das Zielsystem das primäre System ist. Welche Eigenschaften gesperrt sind, ist von der Datenquelle abhängig, aus der die Personenstammdaten importiert wurden.

Detaillierte Informationen zum Thema

- Allgemeine Personenstammdaten auf Seite 128
- Organisatorische Personenstammdaten auf Seite 131
- Adressenangaben für Personen auf Seite 133
- Sonstige Personenstammdaten auf Seite 134

Allgemeine Personenstammdaten

Für Personen erfassen Sie die folgenden allgemeinen Stammdaten. Diese Daten betreffen die persönlichen und die beruflichen Daten einer Person.

Tabelle 35: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Vorname	Vorname der Person.
Nachname	Nachname der Person.
Zweiter Vorname	Zweiter Vorname der Person.
Anrede	Anrede der Person. Die Anrede wird abhängig vom Geschlecht automatisch gebildet.
Titel	Titel der Person.
Namenszusatz	Namenszusatz der Person, beispielsweise **von** oder **zu**.
Bevorzugter Name	Bevorzugter Name der Person.
Initialen	Initialen der Person. Die Initialen werden automatisch aus Vor- und Nachnamen gebildet.
Geschlecht	Geschlecht der Person.
Geburtsdatum	Geburtsdatum der Person.
Geburtsname	Geburtsname der Person.
Berufsbezeichnung	Stellenbezeichnung in Ihrem Unternehmen.
Generationskennzeichen	Zusatz, beispielsweise **Senior** oder **Junior**.
Sprachkultur	Sprache, in der E-Mail-Benachrichtigungen an die Person versendet werden. Die Einstellung wird ebenfalls für die Anzeige des Web Portals genutzt.
Sprache zur Wertformatierung	Sprache zur Darstellung von Werten wie beispielsweise Datumsformate, Zeitformate oder Zahlenformate. Diese Einstellung wird beim Versenden der E-Mail-Benachrichtigungen an die Person berücksichtigt. Die Einstellung

Eigenschaft	Beschreibung
	wird ebenfalls für die Anzeige des Web Portals genutzt.
Unterorganisation	Vermerk, welcher Unterorganisation die Person angehört.
Dauerhaft deaktiviert	Gibt an, ob die Person aktuell ein Mitarbeiter Ihres Unternehmens ist. Ist die Option aktiviert, ist die Person als Mitarbeiter ausgeschieden. Ihr wurden alle Berechtigungen als One Identity Manager Benutzer entzogen. HINWEIS: Personen, die dauerhaft deaktiviert sind, können sich nicht mehr am One Identity Manager anmelden.
Zertifizierungsstatus	Gibt an, ob die Personenstammdaten durch den Manager der Person genehmigt wurden. Der Zertifizierungsstatus wird über Zertifizierungsverfahren gesetzt. Folgende Zertifizierungsstatus sind zulässig. • **Neu**: Die Person wurde neu in der One Identity Manager-Datenbank angelegt. • **Zertifiziert**: Die Personenstammdaten wurden durch einen Manager genehmigt. • **Abgelehnt**: Die Personenstammdaten wurden durch einen Manager nicht genehmigt. Die Person ist dauerhaft deaktiviert.
VIP	Kennzeichnet besonders wichtige Personen.
Sicherheitsgefährdend	Gibt an, ob die Person für Ihr Unternehmen als sicherheitsgefährdend eingestuft ist. Für Personen, die als sicherheitsgefährend eingestuft sind, kann die Vererbung von Ressourcen unterbunden werden. Konfigurieren Sie das Verhalten an den Ressourcen. Für Personen, die als sicherheitsgefährend eingestuft sind, kann die Vererbung von Berechtigungen unterbunden werden. Die Benutzerkonten der Person können gesperrt werden. Die Konfiguration nehmen Sie an den Kontendefinitionen vor. Ausführliche Informationen zu Kontendefinitionen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*. HINWEIS: Personen, die als sicherheitsgefährdend eingestuft sind, können sich nicht mehr am One Identity Manager anmelden. Um die Anmeldung zu erlauben, aktivieren Sie den Konfigurationsparameter **QER | Person | AllowLoginWithSecurityIncident**.
Keine Vererbung	Gibt an, ob die Person Unternehmensressourcen über Rollen

Eigenschaft	Beschreibung
	erbt. Ist die Option aktiviert, wird die Vererbung verhindert. Unternehmensressourcen, die die Person über IT Shop-Bestellungen oder über Systemrollen erhält, werden ebenfalls nicht zugewiesen. Direkte Zuweisungen bleiben bestehen. Wenn der Konfigurationsparameter **QER | Attestation | UserApproval** aktiviert ist, wird die Option in Abhängigkeit der Option **Dauerhaft deaktiviert** gesetzt. Wenn die Person dauerhaft deaktiviert wird, wird über eine Bildungsregel die Option **Keine Vererbung** aktiviert.
Extern	Gibt an, ob die Person interner oder externer Mitarbeiter Ihres Unternehmens ist. Ist die Option aktiviert, ist die Person ein externer Mitarbeiter. In der Standardauslieferung des One Identity Managers sind externe Personen von der automatischen Zuweisung der Kontendefinitionen ausgeschlossen.
Mitarbeitertyp	Genauere Klassifizierung der Person hinsichtlich ihrer vertraglichen Beziehung zum Unternehmen. Zulässig sind **Mitarbeiter**, **Auszubildender**, **Vertragsarbeiter**, **Berater**, **Partner**, **Kunde**, **Andere**.
Kontakt-E-Mail-Adresse	E-Mail-Adresse, an welche bei Erstellung eines neuen Benutzerkontos über das Selbstregistrierungsportal der Registrierungslink gesendet wird.
Firma	Geben Sie eine Firma an. Neue Firmen erfassen Sie über die Schaltfläche neben dem Eingabefeld.
Arbeitsplatz	Arbeitsplatz der Person.
Risikoindex (berechnet)	Für die Risikobewertung einer Person wird anhand der Berechtigungen einer Person ein Risikoindex berechnet. Der Risikoindex einer Person wird aus den Risikoindizes aller ihr zugewiesenen Unternehmensressourcen ermittelt. 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*.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bemerkung	Freitextfeld für zusätzliche Erläuterungen.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Zertifizierungsstatus von Personen ändern auf Seite 143
- Dauerhafte Deaktivierung von Personen auf Seite 139
- Vererbung über Rollen blockieren auf Seite 32
- Berechnung der Zuweisungen auf Seite 23
- Partnerfirmen für externe Personen erstellen und bearbeiten auf Seite 102
- Arbeitsplätze erstellen und bearbeiten auf Seite 187
- Stammdaten für Ressourcen auf Seite 207

Organisatorische Personenstammdaten

Für Personen erfassen Sie die folgenden organisatorischen Stammdaten.

Tabelle 36: Organisatorische Stammdaten

Eigenschaft	Beschreibung
Personalnummer	Personalnummer der Person.
Primäre Abteilung	Abteilung, der die Person primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann die Person über diese Zuordnung ihre Unternehmensressourcen erhalten. Zusätzlich können über die Abteilung die IT Betriebsdaten für Benutzerkonten und Postfächer ermittelt werden.
Primäre Kostenstelle	Kostenstelle, der die Person primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann die Person über diese Zuordnung ihre Unternehmensressourcen erhalten. Zusätzlich können über die Kostenstelle die IT Betriebsdaten für Benutzerkonten und Postfächer ermittelt werden.
Primäre Geschäftsrolle	Geschäftsrolle, der die Person primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann die Person über diese Zuordnung ihre Unternehmensressourcen erhalten. Zusätzlich können über die Geschäftsrolle die IT Betriebsdaten für Benutzerkonten und Postfächer ermittelt werden. HINWEIS: Die Eigenschaft steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.
Sicherheitsmerkmal	Sicherheitskürzel der Person, beispielsweise für Zugangsberechtigungen.

Eigenschaft	Beschreibung
Datum Anlage der Benutzerkonten	Datum, an dem die Benutzerkonten im Zielsystem erzeugt werden sollen. Dieses Datum sollte vor dem Eintrittsdatum liegen. Um Benutzerkonten im One Identity Manager automatisch an diesem Datum zu erzeugen, implementieren Sie unternehmensspezifische Prozesse.
Eintrittsdatum	Datum, an dem die Person ins Unternehmen eingetreten ist. Wird beim Anlegen der Person auf das aktuelle Einfügedatum gesetzt.
Austrittsdatum	Datum, an dem die Person aus dem Unternehmen ausgeschieden ist. Um eine Person und ihre Benutzerkonten zu einem bestimmten Zeitpunkt zu sperren, geben Sie das Austrittsdatum an. Das Austrittsdatum wird durch den Zeitplan **Benutzerkonten ausgeschiedener Personen sperren** regelmäßig überprüft. Bei Erreichen des Austrittsdatums wird die Person gesperrt.
Firmenmitglied	Zusätzliche Informationen zur Firmenzugehörigkeit der Person.
Zeitweilig deaktiviert	Gibt an, ob die Person zeitweilig aus dem Unternehmen ausgeschieden ist. Wenn Sie die Option aktivieren, geben Sie den Zeitraum an, für den die zeitweilige Aktivierung gilt. HINWEIS: Personen, die zeitweilig deaktiviert sind, können sich nicht mehr am One Identity Manager anmelden.
Zeitweilig deaktiviert ab	Datum, ab dem die zeitweilige Deaktivierung gilt.
Zeitweilig deaktiviert bis	Datum, bis zu dem die zeitweilige Deaktivierung gilt. Es ist ein Zeitplan **Zeitweise deaktivierte Benutzerkonten aktivieren** implementiert, der das Enddatum der zeitweiligen Deaktivierung überwacht. Bei Ablauf des Datums werden die Person und ihre Benutzerkonten wieder aktiviert.
Letzter Arbeitstag	Geben Sie das Datum des letzten Arbeitstages an, wenn beispielsweise die Person zu einem bestimmten Tag das Unternehmen verlässt, aber bis zu diesem Tag noch Zugriff auf ihre Daten erhalten soll. HINWEIS: Das Datum des letzten Arbeitstages wird in die Benutzerkonten der Person als Kontoverfallsdatum übernommen. Ein bereits eingetragenes Kontoverfallsdatum im Benutzerkonto wird dabei überschrieben.
Manager	Der Manager einer Person kann innerhalb des One Identity Manager verschiedene Aufgaben wahrnehmen, wie zum Beispiel • Personenstammdaten seiner Mitarbeiter bearbeiten • Personenstammdaten seiner Mitarbeiter zertifizieren

Eigenschaft	Beschreibung
	• Zugewiesene Unternehmensressourcen seiner Mitarbeiter attestieren • Bestellungen seiner Mitarbeiter im IT Shop genehmigen Die Person kann nicht als ihr eigener Manager zugeordnet werden.
Sponsor	Bei der Anlage neuer Personen über das Web Portal können hier zusätzliche Bemerkungen wie beispielsweise der Manager oder Sponsor eingetragen werden.

Verwandte Themen

- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 25
- Dauerhafte Deaktivierung von Personen auf Seite 139
- Zeitweilige Deaktivierung von Personen auf Seite 138

Adressenangaben für Personen

Für ein Person erfassen Sie die folgenden Daten, die den Standort einer Person im Unternehmen beschreiben.

Tabelle 37: Adressangaben

Eigenschaft	Beschreibung
Primärer Standort	Standort, dem die Person primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann die Person über diese Zuordnung ihre Unternehmensressourcen erhalten. Zusätzlich können über den Standort die IT Betriebsdaten für Benutzerkonten und Postfächer ermittelt werden.
Telefon	Telefonnummer der Person.
Mobiltelefon	Mobiltelefonnummer der Person.
Fax	Faxnummer der Person.
Aufnahme in das Telefonbuch	Gibt an, ob die Person im Telefonbuch angezeigt wird.
Straße	Straße.
Gebäude	Gebäude.

Eigenschaft	Beschreibung
Bürobriefkasten	Bürobriefkasten.
Postleitzahl	Postleitzahl.
Ort	Ort.
Land	Land. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln. Diese Angabe ist in der Regel beim Standort oder bei der Abteilung einer Person hinterlegt. Sie können diese Daten jedoch auch bei der Person direkt erfassen. Die Einstellung wird ebenfalls für die Anzeige des Web Portals genutzt.
Bundesland	Bundesland. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln. Diese Angabe ist in der Regel beim Standort oder bei der Abteilung einer Person hinterlegt. Sie können diese Daten jedoch auch bei der Person direkt erfassen.
Etage	Etage.
Raum	Raum.
Bild	Zu einer Person können Sie ein Bild in die Datenbank importieren. Dazu wählen Sie über die Schaltfläche neben dem Eingabefeld den Pfad aus, in dem das Bild zu finden ist.

Verwandte Themen

- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 25
- Ermitteln der Sprache für Personen auf Seite 161
- Ermitteln der Arbeitszeiten für Personen auf Seite 162

Sonstige Personenstammdaten

Für eine Person erfassen Sie die folgenden sonstigen Stammdaten. Diese Daten betreffen die Anmeldung an Zielsystemen, Identitäten, One Identity Manager Anmeldedaten und Daten zu Personenimporten.

Tabelle 38: Sonstige Stammdaten

Eigenschaft	Beschreibung
Zentrales Benutzerkonto	Bezeichnung des One Identity Manager Benutzers. In der Standardinstallation des One Identity Manager wird das zentrale Benutzerkonto aus dem Vornamen und dem Nachnamen der Person gebildet. Das zentrale Benutzerkonto einer Person hat Auswirkungen auf die

Eigenschaft	Beschreibung
	Abbildung der Benutzerkonten in den einzelnen Zielsystemen. Das zentrale Benutzerkonto wird weiterhin bei der Anmeldung an den Werkzeugen des One Identity Manager genutzt.
Zentrales SAP Benutzerkonto	Bezeichnung, die zur Bildung des Benutzerkontos im Zielsystem SAP R/3 herangezogen wird. In der One Identity Manager Standardinstallation wird das zentrale Benutzerkonto aus dem Vornamen und dem Nachnamen der Person gebildet. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das SAP R/3 Benutzermanagement-Modul vorhanden ist.
E-Business Suite Benutzerkonto	Bezeichnung, die zur Bildung des Benutzerkontos im Zielsystem Oracle E-Business Suite herangezogen wird. In der One Identity Manager Standardinstallation wird das E-Business Suite Benutzerkonto aus dem zentralen Benutzerkonto der Person gebildet. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Oracle E-Business Suite Modul vorhanden ist.
E-Business Suite ID	Eindeutige Kennung der HR Person, des AP Kunden, des AP Lieferanten oder des AR Beteiligten in der Oracle E-Business Suite. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Oracle E-Business Suite Modul vorhanden ist.
E-Business Suite Personenkennung	Personalnummer der HR Person in der Oracle E-Business Suite. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Oracle E-Business Suite Modul vorhanden ist.
Zentrales Kennwort und Kennwortbestätigung	Das zentrale Kennwort einer Person kann für die Anmeldung an den Zielsystemen und für die Anmeldung am One Identity Manager verwendet werden. Abhängig von der Konfiguration wird dazu das zentrale Kennwort einer Person an ihre Benutzerkonten und auf ihr Systembenutzerkennwort publiziert. Das zentrale Kennwort kann über das Kennwortrücksetzungsportal geändert werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
Dezentrale Identität und Bestätigung	Kennung der dezentralen Identität zur Identifizierung der Person. Diese Kennung kann für die Anmeldung am One Identity Manager genutzt werden.

Eigenschaft	Beschreibung
Standard-E-Mail-Adresse	Standard-E-Mail-Adresse, um für die Person Postfächer in den einzelnen Zielsystemen zu erstellen. Für die automatische Erzeugung von Postfächern ist diese Angabe zwingend erforderlich. In der One Identity Manager Standardeinstellung wird die Standard-E-Mail-Adresse aus dem zentralen Benutzerkonto des Mitarbeiters und der Standardmaildomäne der aktivierten Zielsysteme gebildet.
Identität	Identitätstyp der Person.
Hauptidentität	Ordnen Sie hier eine Hauptidentität zu, wenn die Person als Subidentität im One Identity Manager geführt wird. Eine Subidentität ermöglicht es Ihnen, spezielle Fälle im One Identity Manager einzurichten. Wenn eine Person mehrere Benutzerkonten in einem Zielsystem hat, die verschiedenen Gruppen zugeordnet werden sollen, sollte für jedes Benutzerkonto eine separate Subidentität mit einem Verweis auf die Hauptidentität eingerichtet werden.
Pseudo-Person	Gibt an, ob die Person eine wirkliche Person darstellt oder eine Pseudo-Person, die beispielsweise für die Verbindung mit administrativen Benutzerkonten genutzt wird.
Wirkliche Person	Eindeutige Kennung der wirklichen Person.
X500-Pseudo-Person	Gibt an, ob die Person als X500-Pseudo-Person im One Identity Manager geführt wird. Hat eine Person mehrere X500-Einträge, die sich in einzelnen Eigenschaften unterscheiden, so können Sie hier ebenfalls Pseudo-Personen nutzen. Für den Anwendungsfall kennzeichnen Sie die Person mit der Option **X500-Pseudo-Person** und stellen eine Verknüpfung zur wirklichen X500-Person her.
X500-Person	Ordnen Sie der X500-Pseudo-Person eine real existierende Person zu.
Anmeldungen	Anmeldungen, mit denen sich die Person an den Werkzeugen des One Identity Manager anmelden kann. Tragen Sie die Anmeldungen in der Form: `Domäne\Benutzer` ein. Diese Informationen werden benötigt, wenn die Authentifizierungsmodule **Benutzerkonto** und **Benutzerkonto (rollenbasiert)** zur Anmeldung an den Werkzeugen des One Identity Manager verwendet werden. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Eigenschaft	Beschreibung
Systembenutzer	Systembenutzer, mit dem sich die Person an den Werkzeugen des One Identity Manager anmelden kann. Die Auswertung der Anmeldedaten erfolgt über das genutzte Authentifizierungsmodul. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
Systembenutzerkennwort und Kennwortbestätigung	Systembenutzerkennwort der Person. Kennwort, mit dem sich die Person an den One Identity Manager-Werkzeugen anmeldet. Das Systembenutzerkennwort kann über das Kennwortrücksetzungsportal geändert werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
Benutzerkontoname (Mainframe)	Wenn die Person mit ihrem Benutzerkonto Zugriff auf dem Mainframe bekommen soll, geben Sie hier den entsprechenden Anmeldenamen an.
Notebook Benutzer	Nur zur Information.
Firmenwagen	Nur zur Information.
Anmeldung am Terminalserver erlaubt	Gibt an, ob der Person die Anmeldung am Terminalserver mit ihrem Benutzerkonto erlaubt ist.
Remote-Zugriff erlaubt	Gibt an, ob sich die Person mit ihrem Benutzerkonto remote in das Netzwerk einwählen darf.
Zurücksetzen des Kennwortes durch Helpdesk erlaubt	Gibt, ob das Zurücksetzen des Kennwortes durch Mitarbeiter des Kennwort-Helpdesk erlaubt ist. Ist diese Option aktiviert, können Mitarbeiter des Kennwort-Helpdesk im Web Portal für Betriebsunterstützung das Kennwort der Person zurücksetzen.
Helpdesk-Mitarbeiter	Gibt an, ob die Person Calls im Helpdesk bearbeiten kann. Ausführliche Informationen zum Helpdesk finden Sie im *One Identity Manager Anwenderhandbuch für das Helpdeskmodul*. HINWEIS: Die Option steht zur Verfügung, wenn das Helpdeskmodul vorhanden ist.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus der die Person importiert wurde. Zusätzlich wird diese Eigenschaft über die Skripte für die automatische Zuordnung von Personen zu Benutzerkonten gesetzt.

Eigenschaft	Beschreibung
Definierter Name	Definierter Name der importierten Person. Diese Eigenschaft sollte durch den Import gesetzt werden.
Kanonischer Name	Vollqualifizierter Name der importierten Person. Diese Eigenschaft sollte durch den Import gesetzt werden.

Verwandte Themen

- Zentrales Benutzerkonto einer Person auf Seite 107
- Zentrales Kennwort einer Person auf Seite 108
- Standard-E-Mail-Adresse einer Person auf Seite 108
- Abbildung mehrerer Identitäten einer Person auf Seite 110
- Identitätstypen von Personen auf Seite 111

Deaktivieren und Löschen von Personen

Der Umgang mit Personen, vor allem beim dauerhaften oder zeitweisen Ausscheiden einer Person aus dem Unternehmen, wird in den einzelnen Unternehmen unterschiedlich gehandhabt. Es gibt Unternehmen, die Personen nie löschen, sondern nur deaktivieren, wenn sie das Unternehmen verlassen.

Detaillierte Informationen zum Thema

- Zeitweilige Deaktivierung von Personen auf Seite 138
- Dauerhafte Deaktivierung von Personen auf Seite 139
- Dauerhaft deaktivierte Personen erneut aktivieren auf Seite 140
- Verzögertes Löschen von Personen auf Seite 141

Zeitweilige Deaktivierung von Personen

HINWEIS: Personen, die zeitweilig deaktiviert sind, können sich nicht mehr am One Identity Manager anmelden.

Die Person ist momentan nicht im Unternehmen, mit der Rückkehr wird zu einem definierten Termin gerechnet. Das gewünschte Verhalten kann sein, dass die Benutzerkonten gesperrt werden und alle Gruppenmitgliedschaften entzogen werden. Oder es sollen die Benutzerkonten gelöscht, bei Wiedereintritt jedoch wieder hergestellt werden, wenn auch mit einer neuen System Identifikationsnummer (SID).

Die zeitweilige Deaktivierung einer Person wird ausgelöst durch:

- die Option **Zeitweilig deaktiviert**
- das Start- und Enddatum der Deaktivierung (**Zeitweilig deaktiviert ab** und **Zeitweilig deaktiviert bis**)

HINWEIS:

- Konfigurieren Sie im Designer den Zeitplan **Benutzerkonten ausgeschiedener Personen sperren**. Dieser Zeitplan prüft das Startdatum der Deaktivierung und setzt bei Erreichen des Startdatums die Option **Zeitweilig deaktiviert**.
- Konfigurieren Sie im Designer den Zeitplan **Zeitweise deaktivierte Benutzerkonten aktivieren**. Dieser Zeitplan überwacht das Enddatum der Deaktivierung und aktiviert bei Ablauf des Datums die Person und ihre Benutzerkonten wieder. Benutzerkonten einer Person, die bereits vor einer zeitweiligen Deaktivierung der Person deaktiviert waren, werden nach Ablauf des Zeitraumes ebenfalls wieder aktiviert.

Verwandte Themen

- Dauerhafte Deaktivierung von Personen auf Seite 139
- Verzögertes Löschen von Personen auf Seite 141

Dauerhafte Deaktivierung von Personen

HINWEIS: Personen, die dauerhaft deaktiviert sind, können sich nicht mehr am One Identity Manager anmelden.

Personen können dauerhaft deaktiviert werden, beispielsweise wenn sie aus dem Unternehmen ausscheiden. Dabei kann es erforderlich sein, dass diesen Personen ihre Berechtigungen in den angeschlossenen Zielsystem und ihre Unternehmensressourcen entzogen werden.

Die Auswirkungen der dauerhaften Deaktivierung einer Person sind:

- Die Person kann nicht als Manager an Personen zugewiesen werden.
- Die Person kann nicht als Verantwortlicher an Rollen zugewiesen werden.
- Die Person kann nicht als Eigentümer an Attestierungsrichtlinien zugewiesen werden.
- Es erfolgt keine Vererbung von Unternehmensressourcen über Rollen, wenn zusätzlich die Option **Keine Vererbung** an der Person aktiviert ist.
- Benutzerkonten der Person werden gesperrt oder gelöscht und den Benutzerkonten werden die Gruppenmitgliedschaften entzogen.

Die dauerhafte Deaktivierung einer Person wird ausgelöst über:

- die Aufgabe **Person dauerhaft deaktivieren**

  Die Aufgabe sorgt dafür, dass die Option **Dauerhaft deaktiviert** aktiviert wird und das Austrittsdatum und das Datum des letzten Arbeitstages auf den aktuellen Tag gesetzt werden.

- das Erreichen des Austrittsdatums

  HINWEIS:

  - Prüfen Sie im Designer den Zeitplan **Benutzerkonten ausgeschiedener Personen sperren**. Dieser Zeitplan prüft das Austrittsdatum und setzt bei Erreichen des Austrittsdatums die Option **Dauerhaft deaktiviert**.
  - Die Aufgabe **Person erneut aktivieren** sorgt dafür, dass die Person wieder aktiviert wird.

- den Zertifizierungsstatus **Abgelehnt**

  Wenn der Zertifizierungsstatus einer Person durch Attestierung oder manuell auf **Abgelehnt** gesetzt wird, wird die Person sofort dauerhaft deaktiviert. Wird der Zertifizierungsstatus auf **Zertifiziert** geändert, wird die Person wieder aktiviert.

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

Verwandte Themen

- Zeitweilige Deaktivierung von Personen auf Seite 138
- Verzögertes Löschen von Personen auf Seite 141
- Dauerhaft deaktivierte Personen erneut aktivieren auf Seite 140
- Zertifizierungsstatus von Personen ändern auf Seite 143

Dauerhaft deaktivierte Personen erneut aktivieren

Dauerhaft deaktivierte Personen können aktiviert werden, wenn Sie nicht durch eine Zertifizierung deaktiviert wurden.

Um eine Person erneut zu aktivieren

1. Wählen Sie im Manager die Kategorie **Personen > Inaktive Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Person erneut aktivieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**, wenn die Person aktiviert werden soll.

Auf dem Stammdatenformular der Person wird die Option **Dauerhaft deaktiviert** deaktiviert. Das Austrittsdatum und das Datum des letzten Arbeitstages werden gelöscht, sofern diese in der Vergangenheit liegen.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Dauerhafte Deaktivierung von Personen auf Seite 139

Verzögertes Löschen von Personen

Beim Löschen einer Person wird geprüft, ob der Person noch Benutzerkonten und Unternehmensressourcen zugeordnet sind oder ob Bestellungen im IT Shop offen sind. Die Person wird zum Löschen markiert und somit für jede weitere Bearbeitung gesperrt.

Standardmäßig werden Personen mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Während dieser Zeit besteht die Möglichkeit die Person wieder zu aktivieren. Nach Ablauf der Löschverzögerung ist ein Wiederherstellen nicht mehr möglich.

Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle `Person`. Ausführliche Informationen zum Konfigurieren der Löschverzögerung finden Sie im *One Identity Manager Konfigurationshandbuch*.

Bevor eine Person endgültig aus der One Identity Manager Datenbank gelöscht werden kann, müssen sämtliche Zuweisungen von Unternehmensressourcen entfernt und Bestellungen abgeschlossen werden. Führen Sie diese Aufgabe manuell durch oder implementieren Sie unternehmensspezifische Prozesse.

Alle mit einer Person verbundenen Benutzerkonten können unter bestimmten Voraussetzung standardmäßig durch den One Identity Manager gelöscht werden, sobald eine Person gelöscht wird. Wenn der Person keine weiteren Unternehmensressourcen zugewiesen sind, wird danach auch die Person endgültig gelöscht.

Verwandte Themen

- Zeitweilige Deaktivierung von Personen auf Seite 138
- Dauerhafte Deaktivierung von Personen auf Seite 139

Löschen aller personenbezogenen Daten

Zur Unterstützung des Sonderprozesses zum Löschen von personenbezogenen Daten (Recht auf Löschung) bei der Umsetzung der Datenschutz-Grundverordnung (DSGVO) wird die Prozedur `QER_PPersonDelete_GDPR` bereitgestellt. Mit dieser Prozedur werden alle personenbezogenen Daten aus der One Identity Manager-Datenbank entfernt. Für einige

Abhängigkeiten werden durch die Prozedur Prozesse erstellt, die durch den One Identity Manager Service verarbeitet werden.

> WICHTIG: Während der Ausführung der Prozedur befindet sich die Datenbank vorübergehend im triggerfreien Zustand. Es wird daher empfohlen, die Prozedur nur in speziellen Wartungsfenstern auszuführen.

Die Prozedur können Sie in einem geeigneten Programm zur Ausführung von SQL Abfragen ausführen.

Aufrufsyntax:

```
exec QER_PPersonDelete_GDPR ' <UID der Person aus der Tabelle Person, Spalte UID_Person>'
```

> HINWEIS: Personenbezogene Daten unterliegen unter Umständen weiteren Regularien wie beispielsweise gesetzlichen Aufbewahrungsfristen. Personenbezogene Daten aus der One Identity Manager History Database werden aus diesem Grund im Standard nicht automatisiert gelöscht. Es wird empfohlen One Identity Manager History Databases entsprechend der Berichtszeiträume zu betreiben. Nach Ablauf eines definierten Berichtszeitraums kann eine neue One Identity Manager History Database eingerichtet werden. Für die Löschung der personenbezogenen Daten richten Sie kundenspezifische Abläufe ein.

Eingeschränkter Zugang zum One Identity Manager

> HINWEIS: Diese Funktion steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Über das Web Portal können sich Benutzer anmelden, die nur zeitweilig oder mit eingeschränkten Berechtigungen Zugriff auf den One Identity Manager bekommen sollen. Diese Funktionalität kann beispielsweise genutzt werden, wenn externen Mitarbeitern zeitweilig Zugang zum One Identity Manager gewährt werden soll. Die Personen können sich am Web Portal als neue Benutzer anmelden. In der One Identity Manager-Datenbank werden für diese Benutzer neue Personenobjekte angelegt.

Wenn Sie diese Funktionalität nutzen, beachten Sie folgende Hinweise:

- Es wird im One Identity Manager eine Person mit folgenden Eigenschaften erstellt:
  - **Zertifizierungsstatus**: Neu
  - **Dauerhaft deaktiviert**: aktiviert
  - **Keine Vererbung**: aktiviert
- Wenn der Konfigurationsparameter **QER | Attestation | UserApproval** aktiviert ist, wird die neue Person automatisch attestiert.
- Um der Person Unternehmensressourcen zuzuweisen oder Berechtigungen im One Identity Manager zu gewähren, implementieren Sie unternehmensspezifische Prozesse.

Ausführliche Informationen zur Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Verwandte Themen

- Zertifizierungsstatus von Personen ändern auf Seite 143

Zertifizierungsstatus von Personen ändern

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

Der Zertifizierungsstatus von Personen wird standardmäßig über die Zertifizierungs- und Rezertifizierungsverfahren gesetzt. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Wenn es erforderlich ist, den Zertifizierungsstatus einer Person außerhalb der regelmäßigen Rezertifizierung zu ändern, können Sie den Status manuell ändern.

Voraussetzung

- Der Konfigurationsparameter **QER | Attestation | UserApproval** ist aktiviert.

Um den Zertifzierungsstatus einer Person manuell zu ändern

1. Um den Zertifizierungsstatus einer aktiven Person zu ändern, wählen Sie im Manager die Kategorie **Personen > Personen**.

   - ODER -

   Um den Zertifizierungsstatus einer dauerhaft deaktivierten Person zu ändern, wählen Sie im Manager die Kategorie **Personen > Inaktive Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Zertifizierungsstatus ändern**.
4. Wählen Sie in der Auswahlliste **Zertifizierungsstatus** den gewünschten Zertifizierungsstatus aus.
5. Um die Änderung zu akzeptieren, klicken Sie **Ok**.

   Auf dem Stammdatenformular der Person wird der neue Zertifizierungsstatus angezeigt.

   HINWEIS: Die Option **Dauerhaft deaktiviert** wird abhängig vom Zertifizierungsstatus aktualisiert. Wird der Zertifizierungsstatus einer Person durch Attestierung oder manuell auf **Abgelehnt** gesetzt, wird die Person sofort dauerhaft deaktiviert. Wird der Zertifizierungsstatus auf **Zertifiziert** geändert, wird die Person aktiviert.

Verwandte Themen

- Eingeschränkter Zugang zum One Identity Manager auf Seite 142
- Dauerhafte Deaktivierung von Personen auf Seite 139

Unternehmensressourcen an Personen zuweisen

Um Unternehmensressourcen zuzuweisen, nutzt der One Identity Manager verschiedene Zuweisungsarten.

- Indirekte Zuweisung

  Bei der indirekten Zuweisung von Unternehmensressourcen werden Personen, Geräte und Arbeitsplätze in Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Anwendungsrollen eingeordnet. Aus der Position innerhalb der Hierarchie, der Vererbungsrichtung (Top-Down, Bottom-Up) und den Unternehmensressourcen, die diesen Rollen zugeordnet sind, berechnet sich die Summe der zugeordneten Unternehmensressourcen für eine Person, ein Gerät oder einen Arbeitsplatz. Bei der indirekten Zuweisung von Unternehmensressourcen wird nochmals zwischen der primären Zuweisung und der sekundären Zuweisung unterschieden.

- Direkte Zuweisung

  Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Person, einem Gerät oder einem Arbeitsplatz. Durch die direkte Zuweisung von Unternehmensressourcen kann ohne weiteren Aufwand auf Sonderanforderungen reagiert werden.

- Zuweisung über dynamische Rollen

  Die Zuweisung über dynamische Rollen ist ein Spezialfall der indirekten Zuweisung. Dynamische Rollen werden eingesetzt, um Rollenmitgliedschaften dynamisch festzulegen. Dabei werden Personen, Geräte oder Arbeitsplätze nicht fest an eine Rolle zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen. Welche Personen, Geräte oder Arbeitsplätze diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Personen einer Abteilung zugewiesen werden; verlässt eine Person diese Abteilung, verliert sie sofort die zugewiesenen Unternehmensressourcen.

- Zuweisung über IT Shop Bestellungen

  Die Zuweisung über IT Shop Bestellungen ist ein Spezialfall der indirekten Zuweisung. Damit Unternehmensressourcen über IT Shop Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Unternehmensressourcen, die als Produkte diesem Shop zugeordnet sind, können von den Kunden bestellt werden. Bestellte Unternehmensressourcen werden nach erfolgreicher Genehmigung den Personen zugewiesen. Neben den

Unternehmensressourcen können über den IT Shop auch Rollenmitgliedschaften bestellt werden.

In der nachfolgenden Tabelle sind die möglichen Zuweisungen von Unternehmensressourcen an Personen dargestellt.

HINWEIS: Die Unternehmensressourcen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 39: Mögliche Zuweisungen von Unternehmensressourcen an Personen

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
Ressourcen	+	+	
Systemrollen	+	+	
Abonnierbare Berichte	+	+	
Software	+	+	
Kontendefinitionen	+	+	
Gruppen kundendefinierter Zielsysteme	-	+	Alle Benutzerkonten kundendefinierter Zielsysteme der Person, für welche die Vererbung von Gruppen zugelassen ist, werden an die Gruppen kundendefinierter Zielsysteme zugewiesen.
Systemberechtigungen kundendefinierter Zielsysteme	-	+	Alle Benutzerkonten kundendefinierter Zielsysteme der Person, für welche die Vererbung von Systemberechtigungen zugelassen ist, werden an die Systemberechtigungen kundendefinierter Zielsysteme zugewiesen.
Active Directory Gruppen	-	+	Alle Active Directory Benutzerkonten und Active Directory Kontakte der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
			die Active Directory Gruppen aufgenommen.
SharePoint Gruppen	-	+	Alle SharePoint Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die SharePoint Gruppen aufgenommen.
SharePoint Rollen	-	+	Alle SharePoint Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die SharePoint Rollen aufgenommen.
LDAP Gruppen	-	+	Alle LDAP Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die LDAP Gruppen aufgenommen.
Notes Gruppen	-	+	Alle Notes Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die Notes Gruppen aufgenommen.
SAP Gruppen	+	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen und für welche die Vererbung von Gruppen zugelassen ist, werden in die SAP Gruppen aufgenommen.
SAP Profile	+	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
			und für welche die Vererbung von Gruppen zugelassen ist, werden in die SAP Profile aufgenommen.
SAP Rollen	+	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen und für welche die Vererbung von Gruppen zugelassen ist, werden in die SAP Rollen aufgenommen.
Strukturelle Profile	-	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen und für welche die Vererbung von Gruppen zugelassen ist, werden in die strukturellen Profile aufgenommen.
BI Analyseberechtigungen	-	+	Alle BI Benutzerkonten der Person, die im selben System liegen und für welche die Vererbung von Gruppen zugelassen ist, erhalten die BI Analyseberechtigungen.
E-Business Suite Berechtigungen	-	+	Alle E-Business Suite Benutzerkonten der Person, die im selben E-Business Suite System liegen und für welche die Vererbung von Gruppen zugelassen ist, werden in die E-Business Suite Gruppen aufgenommen.
Azure Active Directory Gruppen	-	+	Alle Azure Active Directory Benutzerkonten der Person, für welche die Vererbung von Gruppen

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
			zugelassen ist, werden in die Azure Active Directory Gruppen aufgenommen.
Azure Active Directory Administratorrollen	-	+	Alle Azure Active Directory Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die Azure Active Directory Administratorrollen aufgenommen.
Azure Active Directory Abonnements	-	+	Alle Azure Active Directory Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, erhalten die Azure Active Directory Abonnements.
Unwirksamen Azure Active Directory Dienstpläne	-	+	Alle Azure Active Directory Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, erhalten die unwirksamen Azure Active Directory Dienstpläne.
Unix Gruppen	-	+	Alle Unix Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die Unix Gruppen aufgenommen.
PAM Benutzergruppen	-	+	Alle PAM Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die PAM Benutzergruppen aufgenommen.
SharePoint Online Gruppen	-	+	Alle SharePoint Online Benutzerkonten der

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
			Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die SharePoint Online Gruppen aufgenommen.
SharePoint Online Rollen	-	+	Alle SharePoint Online Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die SharePoint Online Rollen aufgenommen.
Google Workspace Produkte und SKUs	-	+	Alle Google Workspace Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die Google Workspace Produkte und SKUs aufgenommen.
Google Workspace Gruppen	-	+	Alle Google Workspace Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die Google Workspace Gruppen aufgenommen.
Cloud Gruppen	-	+	Alle Cloud Benutzerkonten der Person, für welche die Vererbung von Gruppen zugelassen ist, werden an die Cloud Gruppen zugewiesen.
Cloud Systemberechtigungen	-	+	Alle Cloud Benutzerkonten der Person, für welche die Vererbung von Systemberechtigungen zugelassen ist, werden an die Cloud

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
			Systemberechtigungen zugewiesen.

Detaillierte Informationen zum Thema

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 26
- Personen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 150
- Personen an Geschäftsrollen zuweisen auf Seite 151
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88
- Dynamische Rollen auf Seite 37

Personen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Person an Abteilungen, Kostenstellen und Standorte zu, damit die Person über diese Organisationen ihre Unternehmensressourcen erhält. Um Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Organisationen.

Um eine Person an Abteilungen, Kostenstellen und Standorte zuzuweisen (sekundäre Zuweisung; Standardverfahren)

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
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 eine Person an Abteilungen, Kostenstellen oder Standorte zuzuweisen (primäre Zuweisung)

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Tabreiter **Organisatorisch** passen Sie die folgenden Stammdaten an.
    - Primäre Abteilung
    - Primäre Kostenstelle
    - Primärer Standort
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Personen zuweisen auf Seite 144
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88
- Dynamische Rollen auf Seite 37
- Personen in Kundenknoten des IT Shops aufnehmen auf Seite 152
- Personen an Geschäftsrollen zuweisen auf Seite 151
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87

Personen an Geschäftsrollen zuweisen

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

Weisen Sie die Personen an Geschäftsrollen zu, damit die Personen über diese Geschäftsrollen ihre Unternehmensressourcen erhalten. Um Unternehmensressourcen an Geschäftsrollen zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Geschäftsrollen. Ausführliche Informationen zum Arbeiten mit Geschäftsrollen finden Sie im *One Identity Manager Administrationshandbuch für Geschäftsrollen*.

Um eine Person an Geschäftsrollen zuzuweisen (sekundäre Zuweisung; Standardverfahren)

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

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

   Um eine Zuweisung zu entfernen

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

Um eine Person an Geschäftsrollen zuzuweisen (primäre Zuweisung)

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Tabreiter **Organisatorisch** erfassen Sie die primäre Geschäftsrolle.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Personen zuweisen auf Seite 144

Personen in Kundenknoten des IT Shops aufnehmen

Mit der Aufnahme einer Person in einen Kundenknoten ist die Person berechtigt über den IT Shop Bestellungen auszulösen. Auf dem Überblicksformular einer Person werden die Zugriffsberechtigungen auf den IT Shop und die Zuweisungen abgebildet, die sie aufgrund von Produktbestellungen über den IT Shop erhalten hat. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Um eine Person in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **IT Shop-Mitgliedschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** den Kundenknoten zu.

- ODER -

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

5. Speichern Sie die Änderungen.

Anwendungsrollen an eine Person zuweisen

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

Die zugewiesenen Personen erhalten alle Berechtigungen der Berechtigungsgruppe, die der Anwendungsrolle (oder einer übergeordneten Anwendungsrolle) zugeordnet ist. Zusätzlich erhalten die Personen die Unternehmensressourcen, die der Anwendungsrolle zugewiesen sind.

Sind einer Anwendungsrolle keine Personen direkt zugewiesen, dann erhalten die Personen der übergeordneten Anwendungsrolle die Berechtigungen.

HINWEIS: Die Anwendungsrollen **Basisrollen | Jeder (Ändern)**, **Basisrollen | Jeder (Sehen)**, **Basisrollen | Personenverantwortliche** und **Basisrollen | Initiale Berechtigungen** werden automatisch an die Personen zugewiesen. Nehmen Sie keine manuellen Zuweisungen an diese Anwendungsrollen vor.

Um Anwendungsrollen an eine Person zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **One Identity Manager Anwendungsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Anwendungsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Ressourcen direkt an eine Person zuweisen

Ressourcen können direkt oder indirekt an Personen zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Personen und der Ressourcen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einer Person die Ressourcen direkt zuweisen.

Um einer Person Ressourcen direkt zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person aus, der Sie Ressourcen zuweisen wollen.
3. Wählen Sie die Aufgabe **Ressourcen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Ressourcen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Ressourcen direkt an Personen zuweisen auf Seite 211
- Ressourcen verwalten auf Seite 204

Software direkt an Personen zuweisen

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

Software kann direkt oder indirekt an Personen zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Personen und der Software in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Ausführliche Informationen zum Arbeiten mit Software finden Sie im *One Identity Manager Administrationshandbuch für Softwaremanagement*.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einer Person die Software direkt zuweisen.

Um einer Person Software direkt zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person aus, der Sie Software zuweisen wollen.
3. Wählen Sie die Aufgabe **Software zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Software zu.

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

   Um eine Zuweisung zu entfernen

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

Systemrollen direkt an Personen zuweisen

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

Systemrollen können direkt oder indirekt an Personen zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Personen und der Systemrollen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Ausführliche Informationen zum Arbeiten mit Systemrollen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen.*

Um auf Sonderanforderungen schnell zu reagieren, können Sie einer Person die Systemrollen direkt zuweisen.

Um einer Person Systemrollen direkt zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
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.

Abonnierbare Berichte direkt an Personen zuweisen

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

Abonnierbare Berichte können direkt oder indirekt an Personen zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der abonnierbaren Berichte in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Ausführliche Informationen zu abonnierbaren Berichten finden Sie im *One Identity Manager Administrationshandbuch für Berichtsabonnements.*

Um auf Sonderanforderungen schnell zu reagieren, können Sie den Personen die abonnierbaren Berichte auch direkt zuweisen.

Um einer Person abonnierbare Berichte zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Bericht und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Herkunft von Rollen und Berechtigungen von Personen anzeigen

Mit dem Bericht **Herkunft von Berechtigungen anzeigen** können Sie ermitteln, welche Berechtigungen eine Person besitzt und woher diese Berechtigungen stammen. Sie können feststellen, ob eine Person eine Berechtigung direkt oder indirekt erhalten hat. Für die indirekte Zuweisung können Sie ermitteln, ob eine Berechtigung beispielsweise aus einer Abteilungsmitgliedschaft oder einer Bestellung resultiert.

Mit dem Bericht können Sie weiterhin ermitteln, welchen Abteilungen, Kostenstellen, Standorten und Geschäftsrollen eine Person zugewiesen ist und auf welchem Weg diese Mitgliedschaften entstanden sind.

Um den Bericht zur Herkunft zu nutzen

- Aktivieren Sie im Designer den Konfigurationsparameter **SysConfig | Display | SourceDetective** und kompilieren Sie die Datenbank.

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

Um die Herkunft von Berechtigungen für eine Person anzuzeigen

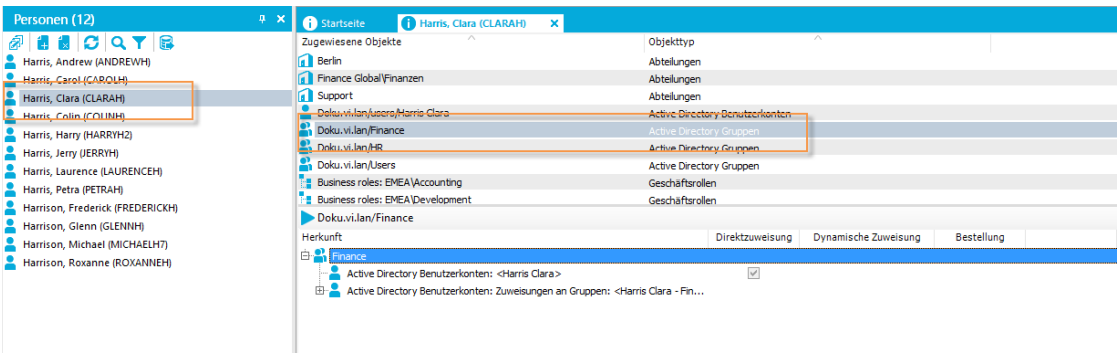
1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste eine Person aus und führen Sie den Bericht **Herkunft von Berechtigungen anzeigen** aus.
3. Im Bereich **Zugewiesene Objekte** sehen Sie die Berechtigungen, Abteilungen, Kostenstellen, Standorte und Geschäftsrollen der Person. Wählen Sie per Maus-Doppelklick einen Eintrag, den Sie genauer betrachten möchten.
4. Im Bereich **Herkunft** werden die Details zum gewählten Eintrag in einer hierarchischen Struktur angezeigt.

Es wird angezeigt, ob es sich um eine direkte Zuweisung, eine dynamische Zuweisung oder eine Bestellung handelt.

- Über die Schaltfläche **Details** können Sie zur dynamischen Rolle oder zur Bestellung wechseln.
- Bei einigen Einträgen der Detailansicht können Sie per Maus-Doppelklick auf das Objekt wechseln.
- Über die Schaltfläche **Untersuchen** können Sie weitere Informationen zur Zuweisung der Berechtigung erhalten.

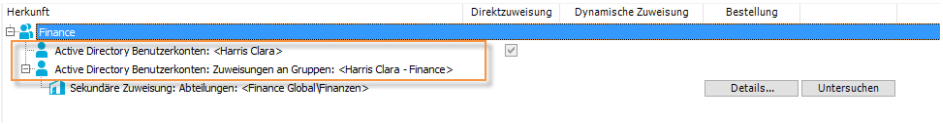
Beispiel: Bericht zur Herkunft einer Berechtigung

Im Bericht **Herkunft von Berechtigungen anzeigen** wird ermittelt, dass Clara Harris der Active Directory Gruppe "Finance" zugewiesen ist.

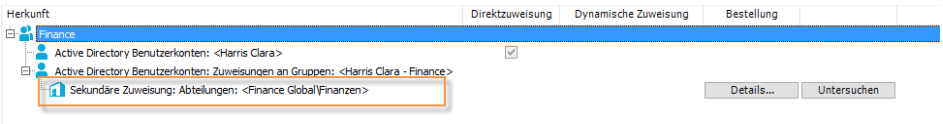


Der Bericht beantwortet verschiedene Fragen.

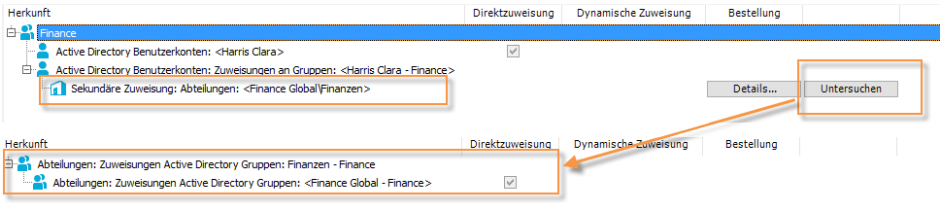
Frage	Warum hat Clara Harris die Active Directory Gruppe "Finance"?
Antwort	Clara Harris besitzt ein Active Directory Benutzerkonto und diesem Benutzerkonto ist die Gruppe "Finance" zugewiesen.



Frage	Warum ist dem Benutzerkonto die Gruppe "Finance" zugewiesen?
Antwort	Clara Harris ist der Abteilung "Finanzen" zugewiesen.

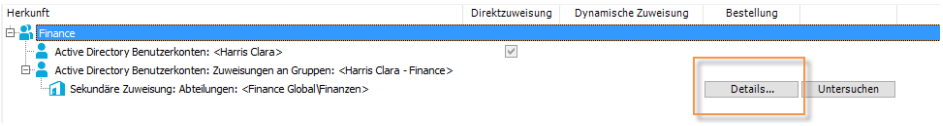


Die Abteilung "Finanzen" erbt von der Abteilung "Finance Global". Der Abteilung "Finance Global" ist die Gruppe "Finance" direkt zugewiesen.



Frage Warum ist Clara Harris in der Abteilung "Finanzen"?

Antwort Es gibt eine Bestellung der Abteilungsmitgliedschaft für Clara Harris.



Analyse von Rollenmitgliedschaften und Zuweisungen an Personen

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

Beispiele:

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

- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

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

Abbildung 13: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 40: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Überblick über Personen anzeigen

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

Um einen Überblick über eine Person zu erhalten

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Überblick über die Person**.

   Auf dem Formular werden die wichtigsten Informationen zu einer Person abgebildet, dazu zählen die Kontaktdaten der Person, die Benutzerkonten und die Zugehörigkeit zu Unternehmensstrukturen. Es werden die zugewiesenen Unternehmensressourcen und der Zugriff auf IT Shop-Strukturen sowie IT Shop-Bestellungen angezeigt.

   Auf dem Formular werden weiterhin die Verantwortlichkeiten der Person innerhalb des One Identity Manager dargestellt. Hierzu zählen die Anwendungsrollen, die einer Person innerhalb des One Identity Manager erhalten hat und die Funktionen als Abteilungsleiter, Kostenstellenverantwortlicher oder Entscheider innerhalb des IT Shops.
4. Wählen Sie die Aufgabe **Überblick über die Berechtigungen der Person**.

   Auf dem Formular werden die Systemberechtigungen und alle Zielsystemgruppen angezeigt, die einer Person zugewiesen sind.

Webauthn-Sicherheitsschlüssel von Personen anzeigen und löschen

One Identity bietet Benutzern die Möglichkeit, sich mithilfe von (physischen) Sicherheitsschlüsseln bequem und sicher an den Webanwendungen des One Identity Managers anzumelden. Diese Sicherheitsschlüssel unterstützen den W3C-Standard **Webauthn**.

Ausführliche Informationen zur Verwendung von Sicherheitsschlüsseln im Web Portal finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*. Ausführliche Informationen zur Konfiguration des Verfahrens finden Sie im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Als Personenadministrator können Sie die Sicherheitsschlüssel von Personen einsehen und bei Bedarf löschen.

Um die Sicherheitsschlüssel einer Person anzuzeigen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Webauthn-Sicherheitsschlüssel anzeigen**.

   Es werden alle Sicherheitsschlüssel der Person angezeigt.
4. Wählen Sie einen Sicherheitsschlüssel in der Liste, um die Details eines einzelnen Sicherheitsschlüssels anzuzeigen.

Um einen Sicherheitsschlüssel einer Person zu löschen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Webauthn-Sicherheitsschlüssel anzeigen**.
4. Wählen Sie den Sicherheitsschlüssel in der Liste und klicken Sie **Entfernen**.
5. Speichern Sie die Änderungen.

Ermitteln der Sprache für Personen

Damit E-Mail Benachrichtigungen, beispielsweise innerhalb eines Bestellprozesses im IT Shop oder bei der Attestierung, in der Sprache des Empfängers verschickt werden können, muss die Sprachkultur der Person ermittelt werden.

- Bundesländer und Länder sowie deren Sprachkulturen sind bereits in der Standardinstallation des One Identity Managers vorhanden. Prüfen und bearbeiten Sie diese Informationen im Designer. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Tragen Sie das Land und das Bundesland am primären Standort, an der primären Abteilung und der primären Kostenstelle, an der primären Geschäftsrolle oder direkt an der Person ein. Für Abbildung von Sonderfällen können Sie die Sprachkultur auch direkt am Standort, an der Abteilung, an der Kostenstelle oder an der Person angeben.

Die Sprache einer Person wird nach folgender Reihenfolge bestimmt:

1. Sprachkultur, die direkt an der Person eingetragen ist.
2. Sprachkultur des Bundeslandes der Person.
3. Sprachkultur des Landes der Person.
4. Sprachkultur, die direkt am primären Standort einer Person eingetragen ist.
5. Sprachkultur des Bundeslandes des primären Standortes.
6. Sprachkultur des Landes des primären Standortes.
7. Sprachkultur, die direkt an der primären Abteilung einer Person eingetragen ist.
8. Sprachkultur des Bundeslandes der primären Abteilung.
9. Sprachkultur des Landes der primären Abteilung.
10. Sprachkultur, die direkt an der primären Kostenstelle einer Person eingetragen ist.
11. Sprachkultur des Bundeslandes der primären Kostenstelle.
12. Sprachkultur des Landes der primären Kostenstelle.
13. Sprachkultur, die direkt an der primären Geschäftsrolle einer Person eingetragen ist.
14. Sprachkultur des Bundeslandes der primären Geschäftsrolle.

15. Sprachkultur des Landes der primären Geschäftsrolle.
16. Fallback, falls nach dieser Reihenfolge keine Sprachkultur ermittelt werden kann:
    a. Sprachkultur aus dem Konfigurationsparameter **Common | MailNotification | DefaultCulture**.
    b. Sprachkultur **en-US**.

Ermitteln der Arbeitszeiten für Personen

Um innerhalb eines Bestellprozesses im IT Shop oder bei der Attestierung Reaktionszeiten von Entscheidern oder Attestierern zu ermitteln, muss die Arbeitszeit der Personen bekannt sein.

- Bundesländer und Länder sowie deren Zeitzonen, Feiertage und übliche Arbeitszeiten sind bereits in der Standardinstallation des One Identity Managers vorhanden. Prüfen und bearbeiten Sie diese Informationen im Designer. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Für die Berechnung der gültigen Arbeitszeit, muss zunächst der Ort (Bundesland oder Land) der Person bestimmt werden. Tragen Sie das Land und das Bundesland am primären Standort, an der primären Abteilung, an der primären Kostenstelle, an der primären Geschäftsrolle oder direkt an der Person ein.
- Anschließend wird die gültige Arbeitszeit berechnet. Bei der Berechnung der gültigen Arbeitszeit werden übliche Arbeitszeiten in den Ländern, Regelungen für Wochenenden und Feiertage sowie unterschiedliche Zeitzonen und Sommerzeit-Regelungen berücksichtigt.

Der Ort einer Person und somit die gültige Arbeitszeit werden nach folgender Reihenfolge bestimmt:

1. Bundesland, das direkt an der Person eingetragen ist.
2. Land, das direkt an der Person eingetragen ist.
3. Bundesland des primären Standortes.
4. Land des primären Standortes.
5. Bundesland der primären Abteilung.
6. Land der primären Abteilung.
7. Bundesland der primären Kostenstelle.
8. Land der primären Kostenstelle.
9. Bundesland der primären Geschäftsrolle.
10. Land der primären Geschäftsrolle.
11. Fallback, falls nach dieser Reihenfolge kein Ort ermittelt werden kann:

a. Bundesland oder Land über die sekundären Standorte, Abteilungen und Kostenstellen.

b. Erstes Land aus allen aktivierten Ländern der Datenbank, sortiert nach Telefonnummer.

c. Land, das als Standard in der Datenbank eingetragen ist (Tabelle `DialogDatabase`, Spalte `UID_DialogCountryDefault`).

   Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

d. Land **USA**.

Benutzerkonten manuell an Personen zuweisen

Auf dem Überblickformular werden alle Benutzerkonten einer Person in den einzelnen Zielsystemen angezeigt. Als Standardverfahren zum Erstellen von Benutzerkonten sollten Sie Kontendefinitionen nutzen. Ausführliche Informationen zu Kontendefinitionen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Um auf Sonderanforderungen zu reagieren, können Sie über die entsprechenden Aufgaben zum Zuweisen von Benutzerkonten manuell ein Benutzerkonto für eine Person zuweisen.

HINWEIS: Die Aufgaben zum manuellen Zuweisen von Benutzerkonten an Personen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind. Weitere Informationen finden Sie in den Handbüchern zu den Zielsystemen.

Verwandte Themen

- Überblick über Personen anzeigen auf Seite 159

Calls für Personen erfassen

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

Über das Helpdeskmodul erfassen Sie Calls für eine Person. Ausführliche Informationen zum Helpdesk finden Sie im *One Identity Manager Anwenderhandbuch für das Helpdeskmodul*.

Um Helpdeskdaten für eine Person zu erfassen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.

3. Wählen Sie die Aufgabe **Calls anzeigen**, um die Calls anzuzeigen, die für eine Person erfasst wurden.
4. Wählen Sie die Aufgabe **Neuer Call**, um einen neuen Call zu erfassen.
5. Speichern Sie die Änderungen.

Zusatzeigenschaften an Personen 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 Person festzulegen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
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.

Verwandte Themen

- Zusatzeigenschaften erstellen und bearbeiten auf Seite 222

Berichte über Personen

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 Personen stehen folgende Berichte zur Verfügung.

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

Tabelle 41: Berichte zur über Personen

Bericht	Beschreibung
Herkunft von Berechtigungen	Der Bericht zeigt die Berechtigungen und Rollen einer Person und die möglichen Zuweisungswege an.
Bestellhistorie	Über den Bericht erhalten Sie einen Überblick über die einzelnen IT Shop Bestellungen einer Person. Der Bericht unterteilt nach genehmigten, abbestellten, abgelehnten und offenen Bestellungen. Für jedes bestellte Produkt ist nachvollziehbar, wann und warum es bestellt, verlängert oder abbestellt wurde. Für abgeschlossene Bestellungen zeigen Sie über die Schaltfläche **Anzeigen** die Genehmigungshistorie an. In der Genehmigungshistorie sehen Sie den Entscheidungsworkflow, die Ergebnisse der einzelnen Entscheidungsschritte und die Entscheider. Für offene Bestellungen sehen Sie über die Schaltfläche **Anzeigen** den aktuellen Entscheidungsverlauf.
Datenqualität der verantworteten Personen	Der Bericht wertet die Datenqualität der Personendatensätze aus. Berücksichtigt werden alle Personen des Verantwortungsbereiches.
Personen pro Abteilung	Der Bericht enthält die Anzahl der Personen pro Abteilung. Berücksichtigt werden die primären und sekundären Zuweisungen der Personen zu den Organisationen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.
Personen pro Kostenstelle	Der Bericht enthält die Anzahl der Personen pro Kostenstelle. Berücksichtigt werden die primären und sekundären Zuweisungen der Personen zu den Organisationen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.
Personen pro Standort	Der Bericht enthält die Anzahl der Personen pro Standort. Berücksichtigt werden die primären und sekundären Zuweisungen der Personen zu den Organisationen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.
Datenqualität der Personendatensätze	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität aller Personen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.
Berechtigungsüberblick zu einem definierten Zeitpunkt	Der Bericht enthält detaillierte Informationen über persönliche und organisatorische Daten sowie einen Überblick über alle Unternehmensressourcen, welche die Person zu einem bestimmten Zeitpunkt besaß. Das umfasst alle zugewiesenen Benutzerkonten, Systemberechtigungen, Rollen, Kontendefinitionen, Ressourcen und Software.
Attestierungsvorgänge	Der Bericht zeigt abgeschlossene und offene Attes-

Bericht	Beschreibung
	tierungsvorgänge, für welche die Person als Attestierer ermittelt wurde. Wenn die Person am Manager angemeldet ist, kann sie über den Bericht die Attestierungsvorgänge genehmigen oder ablehnen. Über die Optionen **Genehmigen** oder **Ablehnen** geben Sie Ihre Entscheidung ein. Tragen Sie unter **Begründung der Entscheidung** die Begründung ein und klicken Sie auf die Schaltfläche **Entscheidung ausführen**. Wurde für den Attestierungsvorgang ein Bericht definiert, können Sie diesen über die Schaltfläche in der Spalte **Bericht anzeigen** einsehen. Über die Aufgabe **Attestierungshistorie anzeigen** werden die einzelnen Schritte des Attestierungsvorgangs dargestellt. Sie können hier den zeitlichen Ablauf und die Entscheidungen im Attestierungsvorgang nachvollziehen. Die Attestierungshistorie wird sowohl für offene als auch für abgeschlossene Attestierungen angezeigt. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Übersicht mit Rollen und Benutzerkonten	Der Bericht enthält detaillierte Informationen über persönliche und organisatorische Daten sowie der Person aktuell zugewiesene Benutzerkonten, Rollen und Berechtigungen. Sie können entscheiden, ob abhängige Identitäten in den Bericht einbezogen werden sollen.
Übersicht mit Rollen und Benutzerkonten (inklusive Historie)	Der Bericht enthält detaillierte Informationen über persönliche und organisatorische Daten sowie der Person aktuell zugewiesene Benutzerkonten, Rollen und Berechtigungen, einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt. Sie können entscheiden, ob abhängige Identitäten in den Bericht einbezogen werden sollen. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Zielsystem Basismodul vorhanden ist.
Übersicht der direkt verantworteten Personen	Der Bericht zeigt alle Personen in direkter Verantwortung. Detaillierte Informationen über persönliche und organisatorische Daten sowie aktuelle Benutzerkonten, Rollen und Berechtigungen werden dargestellt. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Zielsystem Basismodul vorhanden ist.

Bericht	Beschreibung
Übersicht der verant-worteten Personen (inklusive Historie)	Der Bericht zeigt alle Personen des Verantwortungsbereichs. Detaillierte Informationen über persönliche und organisatorische Daten sowie aktuelle Benutzerkonten, Rollen und Berechtigungen werden dargestellt, einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten anzeigen (inklusive Historie)	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen, einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Zielsystem Basismodul vorhanden ist.
Benutzerkonten von direkt verantworteten Personen (inklusive Historie)	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen, einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Zielsystem Basismodul vorhanden ist.
Übersicht der eigenen Systemberechtigungen (inklusive Historie)	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten, einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Zielsystem Basismodul vorhanden ist.
Übersicht über den privilegierten Zugriff der Person	Der Bericht enthält detaillierte Informationen über persönliche und organisatorische Daten sowie die aktuellen privilegierten Zugriffe der Person. HINWEIS: Dieser Bericht steht zur Verfügung, wenn das Privileged Account Governance Modul vorhanden ist.

Verwandte Themen

- Herkunft von Rollen und Berechtigungen von Personen anzeigen auf Seite 156
- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 158

Geräte und Arbeitsplätze verwalten

Der One Identity Manager bietet eine erweiterte Funktionalität in der Geräteverwaltung für ein Netzwerk. Der One Identity Manager unterscheidet zwischen Gerätetypen, Gerätemodellen und Geräten an sich.

- Gerätetypen, wie beispielsweise PC, Drucker oder Monitor, dienen einer ersten Klassifizierung der Geräte.
- Gerätemodelle dienen der weiteren Verfeinerung der Gerätetypen, um eine genauere Klassifizierung der Geräte vornehmen zu können.
- Unter Geräte werden die konkreten Geräte, wie sie im Netz vorhanden sind, definiert.

Arbeitsplätze dienen der Zuordnung von verschiedenen Geräten zu einer Arbeitsstation. Über die Einordnung von Arbeitsplätzen in Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder dynamische Rollen können Sie die Zuweisung von Unternehmensressourcen weitgehend automatisieren.

Um Geräte und Arbeitsplätze im One Identity Manager zu verwalten

- Aktivieren Sie im Designer den Konfigurationsparameter **Hardware** und kompilieren Sie die Datenbank.

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

Detaillierte Informationen zum Thema

Basisdaten für die Geräteverwaltung

Für die Geräteverwaltung werden die folgenden Basisdaten benötigt.

- 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**.
- Gerätemodelle

  Gerätemodelle werden benötigt um eine Klassifizierung der Geräte vornehmen zu können, beispielsweise PC, Server, Monitor, Drucker. Der One Identity Manager enthält vordefinierte Gerätemodelle.
- Angaben zu Herstellern und Lieferanten

  Für die Erfassung von Gerätemodellen und Geräten können Sie Herstellerfirmen und Lieferantenfirmen hinterlegen.
- Gerätestatus

  Für die Anlageinformationen zu Geräten erfassen Sie die möglichen Gerätestatus.
- Arbeitsplatzstatus

  Arbeitsplätze können Sie mit einem Status versehen.
- Arbeitsplatztypen

  Zur weiteren Klassifizierung von Arbeitsplätzen erfassen Sie Arbeitsplatztypen.

Detaillierte Informationen zum Thema

- Gerätemodelle erstellen und bearbeiten auf Seite 171
- Partnerfirmen erstellen und bearbeiten auf Seite 173
- Gerätestatus erstellen und bearbeiten auf Seite 175
- Arbeitsplatzstatus erstellen und bearbeiten auf Seite 175
- Arbeitsplatztypen erstellen und bearbeiten auf Seite 176
- Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen auf Seite 233

Gerätemodelle erstellen und bearbeiten

Voraussetzung für das Anlegen von Geräten ist die Definition von Gerätemodellen. Gerätemodelle werden benötigt um eine Klassifizierung der Geräte vornehmen zu können, beispielsweise PC, Server, Monitor, Drucker. Der One Identity Manager enthält vordefinierte Gerätemodelle. Sie können weitere Gerätemodelle definieren.

Um ein Gerätemodell zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Gerätemodelle**.
2. Wählen Sie in der Ergebnisliste ein Gerätemodell und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Gerätemodelle auf Seite 171
- Inventurdaten für Gerätemodelle auf Seite 172

Allgemeine Stammdaten für Gerätemodelle

Für ein Gerätemodell erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 42: Stammdaten eines Gerätemodells

Eigenschaft	Beschreibung
Gerätemodell	Bezeichnung des Gerätemodells.
Gerätetyp	Typ des Gerätes. Über den Gerätetyp eines Gerätemodells werden bei Einrichtung eines neuen Gerätes die angebotenen Formulare zur Stammdatenpflege gefiltert.
Firma	Herstellerfirma. Neue Firmen erfassen Sie über die Schaltfläche neben dem Eingabefeld. Weitere Informationen finden Sie unter Partnerfirmen erstellen und bearbeiten auf Seite 173. HINWEIS: Als Firmen werden nur die als Hersteller markierten Firmen zur Auswahl angeboten. Bei Neuanlage eines Gerätes wird die hinterlegte Firma des Gerätemodells als Hersteller übernommen.

Eigenschaft	Beschreibung
Leistungsposition	Wenn Sie dem Gerätemodell eine Leistungsposition zuweisen, kann die Nutzung eines Gerätemodells intern abgerechnet werden. Neue Leistungspositionen erfassen Sie über die Schaltfläche neben dem Eingabefeld.
Webseite	Webseite des Herstellers. Über die Schaltfläche wird die angegebene Herstellerseite im Standardwebbrowser angezeigt.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Zusätzliche Daten	Freitextfeld für zusätzliche Erläuterungen.
PC	Gibt an, ob das Gerät prinzipiell als PC im Sinne einer Arbeitsstation einsetzbar ist.
Server	Gibt an , ob das Gerät als Server eingesetzt werden soll.
Lokaler Peripherie	Gibt an, ob es sich bei diesem Gerätetyp um eine lokale Peripherie handelt, die an einen PC angeschlossen werden kann.
Deaktiviert	Gibt an, ob das Gerätemodell verwendet wird oder nicht mehr im Einsatz ist. HINWEIS: Nur Gerätemodelle, die aktiviert sind, können innerhalb des One Identity Manager zugewiesen werden. Ist ein Gerätemodell deaktiviert, dann wird die Zuweisung des Gerätemodells unterbunden, bereits bestehende Zuweisungen bleiben jedoch erhalten.

Inventurdaten für Gerätemodelle

Zu einem Gerätemodell können Sie die folgenden Inventurdaten und kaufmännische Informationen erfassen.

HINWEIS: Die Angabe der Preise erfolgt standardmäßig mit 2 Nachkommastellen. Die Anzahl der anzugebenden Kommastellen kann im Designer unternehmensspezifisch angepasst werden. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Tabelle 43: Inventurdaten für ein Gerätemodell

Eigenschaft	Beschreibung
Standard-Lieferant	Lieferantenfirma. Weitere Informationen finden Sie unter Partnerfirmen erstellen und bearbeiten auf Seite 173.
Person	Person, die für den Kauf zuständig ist.
Alternatives Gerätemodell	Alternatives Gerätemodell.

Eigenschaft	Beschreibung
Garantie[Monate]	Standardgarantie des Herstellers in Monaten.
Zusätzliche Garantie [Monate]	Zusatzgarantie des Herstellers in Monaten.
Verwendung [Monate]	Vorgesehene Nutzungsdauer in Monaten.
Mindestbestand	Erforderlicher Mindestbestand im Lager.
Max. Bestand	Höchstbestand im Lager.
Positionsnummer	Artikelnummer beim Lieferanten.
Bestelleinheit	Maßeinheit für Bestellungen.
Mindestbestellmenge	Mindestmenge bei Bestellungen.
Datum des letzten Angebotes	Datum des letzten Angebotes.
Preis des letzten Angebotes	Preis des letzten Angebotes.
Datum der letzten Lieferung	Datum der letzten Lieferung.
Preis der letzten Lieferung	Preis der letzten Lieferung.

Partnerfirmen erstellen und bearbeiten

Erfassen Sie die Angaben zu externen Firmen, die als Hersteller, Lieferanten oder Leasinggeber auftreten können.

Um eine Partnerfirma zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Partnerfirmen**.
2. Wählen Sie in der Ergebnisliste eine Firma und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Erfassen Sie die folgenden Stammdaten für eine Firma.

Tabelle 44: Allgemeine Stammdaten einer Firma

Eigenschaft	Beschreibung
Firma	Kurzbezeichnung der Firma für die Anzeige in den One Identity Manager-Werkzeugen.
Bezeichnung	Vollständige Bezeichnung der Firma.
Namenszusatz	Ergänzung zur Bezeichnung der Firma.
Kurzname	Kurzname der Firma.
Kontakt	Ansprechpartner der Firma.
Partner	Gibt an, ob es sich um eine Partnerfirma handelt.
Kundennummer	Kundennummer bei der Partnerfirma.
Lieferant	Gibt an, ob es sich um einen Lieferanten handelt.
Kundennummer	Kundennummer beim Lieferanten.
Leasing-Partner	Gibt an, ob es sich um einen Leasinggeber oder Vermieter handelt.
Hersteller	Gibt an, ob es sich um eine Herstellerfirma handelt.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.

Tabelle 45: Adressdaten einer Firma

Eigenschaft	Beschreibung
Straße	Straße.
Gebäude	Gebäude.
Postleitzahl	Postleitzahl.
Ort	Ort.
Bundesland	Bundesland.
Land	Land.
Telefon	Telefonnummer der Firma.
Fax	Faxnummer der Firma.
E-Mail-Adresse	E-Mail-Adresse der Firma.
Webseite	Webseite der Firma. Über die Schaltfläche wird die angegebene Webseite im Standardwebbrowser angezeigt.

Gerätestatus erstellen und bearbeiten

Erfassen Sie die Status, welche die Geräte annehmen können beispielsweise Aktiv, Inaktiv, Einlagerung.

Um einen Gerätestatus zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Gerätestatus**.
2. Wählen Sie in der Ergebnisliste einen Gerätestatus und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Erfassen Sie die folgenden Stammdaten für einen Gerätestatus.

Tabelle 46: Stammdaten eines Gerätestatus

Eigenschaft	Beschreibung
Gerätestatus	Bezeichnung des Gerätestatus.
Kurzbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Arbeitsplatzstatus erstellen und bearbeiten

Erfassen Sie die Status, welche die Arbeitsplätze annehmen können beispielsweise Aktiv, Inaktiv, Einlagerung.

Um einen Arbeitsplatzstatus zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Arbeitsplatzstatus**.
2. Wählen Sie in der Ergebnisliste einen Arbeitsplatzstatus und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Erfassen Sie die folgenden Stammdaten für einen Arbeitsplatzstatus.

Tabelle 47: Stammdaten eines Arbeitsplatzstatus

Eigenschaft	Beschreibung
Status	Bezeichnung des Arbeitsplatzstatus.
Kurzbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Arbeitsplatztypen erstellen und bearbeiten

Zur weiteren Klassifizierung von Arbeitsplätzen erfassen Sie Arbeitsplatztypen. Erfassen Sie zusätzliche Gerätevoraussetzungen für einen Arbeitsplatz.

Um einen Arbeitsplatztyp zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Arbeitsplatztyp**.
2. Wählen Sie in der Ergebnisliste einen Arbeitsplatztyp und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Erfassen Sie die folgenden Stammdaten für einen Arbeitsplatztyp.

Tabelle 48: Stammdaten eines Arbeitsplatztyp

Eigenschaft	Beschreibung
Arbeitsplatztyp	Bezeichnung des Arbeitsplatztyp.
Anzeigename	Bezeichnung zur Anzeige in den One Identity Manager-Werkzeugen.
Kurzbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Leasingrate	Leasingrate.
Diskettenlaufwerk notwendig	Gibt an, ob an diesem Arbeitsplatztyp ein Diskettenlaufwerk benötigt wird.
CD-Laufwerk notwendig	Gibt an, ob an diesem Arbeitsplatztyp ein CD-Laufwerk benötigt wird.

Geräte erstellen und bearbeiten

Tabelle 49: Konfigurationsparameter für die Einrichtung eines Gerätes

Konfigurationsparameter	Wirkung bei Aktivierung
Hardware | Display | CustomHardwareType	Beim Einrichten eines neuen Gerätes mit dem entsprechenden Gerätemodell werden auf die Stammdaten angepasste Formulare angezeigt.
Hardware | Display | CustomHardwareType | MobilePhone	Angabe des Gerätetyps, der ein Mobiltelefone repräsentiert.
Hardware | Display | CustomHardwareType | Monitor	Angabe des Gerätetyps, der einen Monitor repräsentiert.
Hardware | Display | CustomHardwareType | PC	Angabe des Gerätetyps, der einen PC repräsentiert.
Hardware | Display | CustomHardwareType | Printer	Angabe des Gerätetyps, der einen Drucker repräsentiert.
Hardware | Display | CustomHardwareType | Server	Angabe des Gerätetyps, der einen Server repräsentiert.
Hardware | Display | CustomHardwareType | Tablet	Angabe des Gerätetyps, der ein Tablet repräsentiert.
Hardware | Display | MachineWithRPL	Die Angaben zum Remote Boot für Arbeitsstationen und Server sind bearbeitbar.
Hardware | Workdesk | WorkdeskAuto	Bei Einrichtung einer Arbeitsstation oder eines Servers wird automatisch ein zugehöriger Arbeitsplatz erzeugt.

Mit dem One Identity Manager können Sie verschiedene Geräte, wie beispielsweise Arbeitsstationen, Server, Monitore, Drucker oder sonstige Geräte, verwalten.

Um ein Gerät zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Geräte**.
2. Wählen Sie einen der folgenden Filter.
    - Personal Computer
    - Server
    - Monitore

- Drucker
- Mobiltelefone
- Tablets
- Sonstige

Abhängig vom gewählten Filter wird beim Einfügen eines neuen Gerätes das Gerätemodell bestimmt und das entsprechende Formular zum Bearbeiten der Stammdaten ermittelt.

3. Wählen Sie in der Ergebnisliste ein Gerät und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste  .
4. Bearbeiten Sie die Stammdaten des Gerätes.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Geräte auf Seite 178
- Netzwerkinformationen für Geräte auf Seite 181
- Anlageinformationen für Geräte auf Seite 198
- Unternehmensressourcen an Geräte zuweisen auf Seite 182

Allgemeine Stammdaten für Geräte

Für ein Gerät erfassen Sie die folgenden allgemeinen Stammdaten. Die verfügbaren Stammdaten sind abhängig vom gewählten Gerätemodell.

Tabelle 50: Allgemeine Stammdaten eines Gerätes

Eigenschaft	Beschreibung
Anlagegut Nummer	Nummer des Anlagegutes in der Anlagenbuchhaltung.
Gerätekennung	Eindeutige Kennung des Gerätes.
PC	Gibt an, ob es sich um einen Computer handelt.
Server	Gibt an, ob es sich um einen Server handelt.
Lokale Peripherie	Gibt an, ob es sich um lokale Peripheriegeräte handelt, beispielsweise Monitor, Drucker und ein sonstiges Peripheriegerät.
Hersteller	Herstellerfirma.

Eigenschaft	Beschreibung
Gerätemodell	Bezeichnung des Gerätemodells. Die verfügbaren Stammdaten sind abhängig vom gewählten Gerätemodell.
Gerätestatus	Status der Geräte.
Arbeitsplatz	Arbeitsplatz des Gerätes. Der Arbeitsplatz dient zur Zuordnung von verschiedenen Geräten zu einer Arbeitsstation oder einem Server. Ist der Konfigurationsparameter **Hardware | Workdesk | WorkdeskAuto** aktiviert, wird beim Einrichten einer Arbeitsstation oder eines Servers automatisch ein gleich bezeichneter Arbeitsplatz angelegt.
Übergeordnetes Gerät	Übergeordnetes Gerät, mit dem dieses Gerät verknüpft ist.
VM Client (Option)	Gibt an, ob das Gerät eine virtuelle Maschine ist.
VM Host	Gerät, auf der die virtuelle Maschine installiert ist. Die Auswahl wird freigeschaltet, wenn die Option **VM Client** aktiviert wird.
VM Host (Option)	Gibt an, ob es sich um einen Host für virtuelle Maschinen handelt.
Telefon	Telefonnummer.
Verwendet von	Person, die dieses Gerät benutzt.
Primäre Abteilung	Abteilung, der das Gerät primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten.
Primärer Standort	Standort, dem das Gerät primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten.
Primäre Kostenstelle	Kostenstelle, der das Gerät primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten.
Primäre Geschäftsrolle	Geschäftsrolle, der das Gerät primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann das Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten. HINWEIS: Die Eigenschaft steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.
Investition	Investitionen oder Investitionsvorhaben zum Gerät.

Eigenschaft	Beschreibung
Standortbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Keine Vererbung	Gibt an, ob das Gerät Unternehmensressourcen über Rollen erbt. Ist die Option aktiviert, wird die Vererbung verhindert. Direkte Zuweisungen bleiben bestehen.
Betriebssystem	Bezeichnung des Betriebssystems.
Version Betriebssystem	Version des Betriebssystems.
Servicepack Betriebs-system	Bezeichnung des Servicepacks.
Hotfix Betriebssystem	Bezeichnung des Hotfixes.
Netzbetreiber	Netzbetreibervertrag für das Gerät.
Seriennummer	Seriennummer des Herstellers.
MAC-Adresse	MAC-Adresse des Gerätes.
IMEI	IMEI-Nummer des Gerätes.
ICCID	ICCID-Nummer des Gerätes.
Bios Version	Version des BIOS.
Anzahl Prozessoren	Anzahl der Prozessoren im Gerät.
RAM [MB]	RAM in Megabyte.
1. HDD Kapazität [MB]	Kapazität der 1. Platte in Megabyte.
2. HDD Kapazität [MB]	Kapazität der 2. Platte in Megabyte.
Max. Auflösung vertikal	Maximale senkrechte Bildauflösung.
Max. Auflösung horizon-tal	Maximale waagerechte Bildauflösung.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Gerätemodelle erstellen und bearbeiten auf Seite 171
- Partnerfirmen erstellen und bearbeiten auf Seite 173

- Gerätestatus erstellen und bearbeiten auf Seite 175
- Anlageinformationen für Geräte auf Seite 198
- Investitionen und Investitionsvorhaben für Geräte erfassen auf Seite 200
- Arbeitsplätze erstellen und bearbeiten auf Seite 187
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Vererbung an einzelne Personen, Geräte oder Arbeitsplätze verhindern auf Seite 34

Netzwerkinformationen für Geräte

Für die Netzwerkkonfiguration erfassen Sie die folgenden Informationen. Die verfügbaren Stammdaten sind abhängig vom gewählten Gerätemodell.

Tabelle 51: Netzwerkinformationen

Eigenschaft	Beschreibung
IP-Adresse (IPv4)	IP Adresse im IPv4 Format.
IP-Adresse (IPv6)	IP Adresse im IPv6 Format.
DHCP benutzen	Gibt an, ob die IP-Adressen von einem DHCP Server bezogen werden. Ist die Option nicht aktiviert, vergeben Sie eine feste IP-Adresse und erfassen die Subnetz-Maske und Standard-Gateway.
Subnet-Maske	Subnetz-Maske.
Standard-Gateway	Standard-Gateway.
WINS benutzen	Gibt an, ob WINS zur Namensauslösung genutzt wird. Ist die Option aktiviert, geben Sie die IP-Adressen des bevorzugten und des alternativen WINS-Servers an.
WINS primär	IP-Adresse des bevorzugten WINS Servers.
WINS sekundär	IP-Adresse des alternativen WINS Servers.
Bereichs-ID	Um miteinander zu kommunizieren, benötigen alle Computer eines TCP-/IP-Netzwerkes dieselbe Bereichs-ID. Die Bereichs-ID wird zur Identifikation genutzt, wenn der angegebene DNS Server nicht gefunden werden kann. Im Normalfall ist die Angabe leer zu lassen.
DNS benutzen	Gibt an, ob DNS zur Namensauflösung eingesetzt wird. Ist die Option aktiviert, geben Sie die IP-Adressen des bevorzugten und des alternativen DNS-Servers an.

Eigenschaft	Beschreibung
DNS Server	IP-Adresse des bevorzugten DNS Servers.
2. DNS Server	IP-Adresse des alternativen DNS Servers.
3. DNS Server	IP-Adresse des alternativen DNS Servers.
DNS Name	DNS-Suffix der Domäne, der das Gerät angehört.
DNS Hostname	DNS-Name des Computers.
Remote Boot	Gibt an, ob dieses Gerät Remote-Boot nutzt. Die Eigenschaft steht zur Verfügung, wenn der Konfigurationsparameter **Hardware | Display | MachineWithRPL** aktiviert ist.
Remote Boot Typ	Angabe des Remote Boot Typs. Die Eigenschaft steht zur Verfügung, wenn der Konfigurationsparameter **Hardware | Display | MachineWithRPL** aktiviert ist.

Unternehmensressourcen an Geräte zuweisen

Um Unternehmensressourcen zuzuweisen, nutzt der One Identity Manager verschiedene Zuweisungsarten.

- Indirekte Zuweisung

  Bei der indirekten Zuweisung von Unternehmensressourcen werden Personen, Geräte und Arbeitsplätze in Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Anwendungsrollen eingeordnet. Aus der Position innerhalb der Hierarchie, der Vererbungsrichtung (Top-Down, Bottom-Up) und den Unternehmensressourcen, die diesen Rollen zugeordnet sind, berechnet sich die Summe der zugeordneten Unternehmensressourcen für eine Person, ein Gerät oder einen Arbeitsplatz. Bei der indirekten Zuweisung von Unternehmensressourcen wird nochmals zwischen der primären Zuweisung und der sekundären Zuweisung unterschieden.

- Direkte Zuweisung

  Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Person, einem Gerät oder einem Arbeitsplatz. Durch die direkte Zuweisung von Unternehmensressourcen kann ohne weiteren Aufwand auf Sonderanforderungen reagiert werden.

- Zuweisung über dynamische Rollen

  Die Zuweisung über dynamische Rollen ist ein Spezialfall der indirekten Zuweisung. Dynamische Rollen werden eingesetzt, um Rollenmitgliedschaften dynamisch festzulegen. Dabei werden Personen, Geräte oder Arbeitsplätze nicht fest an eine Rolle zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen.

Welche Personen, Geräte oder Arbeitsplätze diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Personen einer Abteilung zugewiesen werden; verlässt eine Person diese Abteilung, verliert sie sofort die zugewiesenen Unternehmensressourcen.

In der nachfolgenden Tabelle sind die möglichen Zuweisungen von Unternehmensressourcen an Geräte dargestellt.

HINWEIS: Die Unternehmensressourcen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 52: Mögliche Zuweisungen von Unternehmensressourcen an Geräte

Unternehmensressourcen	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
Active Directory Gruppen	-	+	Alle Active Directory Computer, die dieses Gerät referenzieren, werden in die Active Directory Gruppen aufgenommen.
LDAP Gruppen	-	+	Alle LDAP Computer, die dieses Gerät referenzieren, werden in die LDAP Gruppen aufgenommen.

HINWEIS: Zusätzlich erhalten die Geräte die Unternehmensressourcen ihres Arbeitsplatzes.

Detaillierte Informationen zum Thema

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 26
- Geräte an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 184
- Geräte an Geschäftsrollen zuweisen
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88

- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 190
- Dynamische Rollen auf Seite 37

Geräte an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie das Gerät an Abteilungen, Kostenstellen und Standorte zu, damit das Gerät über diese Organisationen seine Unternehmensressourcen erhält. Um Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Organisationen.

Um ein Gerät an Abteilungen, Kostenstellen und Standorte zuzuweisen (sekundäre Zuweisung; Standardverfahren)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Geräte > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
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 ein Gerät an Abteilungen, Kostenstellen oder Standorte zuzuweisen (primäre Zuweisung)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Geräte > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Passen Sie die folgenden Stammdaten an.
   - **Primäre Abteilung**: Abteilung, der das Gerät zugewiesen wird.
   - **Primäre Kostenstelle**: Kostenstelle, der das Gerät zugewiesen wird.
   - **Primärer Standort**: Standort, dem das Gerät zugewiesen wird.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Geräte zuweisen auf Seite 182
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88
- Dynamische Rollen auf Seite 37
- Personen an Geschäftsrollen zuweisen auf Seite 151
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87

Geräte an Geschäftsrollen zuweisen

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

Weisen Sie das Gerät an Geschäftsrollen zu, damit das Gerät über diese Geschäftsrollen seine Unternehmensressourcen erhält. Um Unternehmensressourcen an Geschäftsrollen zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Geschäftsrollen. Ausführliche Informationen zum Arbeiten mit Geschäftsrollen finden Sie im *One Identity Manager Administrationshandbuch für Geschäftsrollen*.

Um ein Gerät an Geschäftsrollen zuzuweisen (sekundäre Zuweisung; Standardverfahren)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um ein Gerät an Geschäftsrollen zuzuweisen (primäre Zuweisung)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie in der Auswahlliste **Primäre Geschäftsrolle** die Geschäftsrolle, der das Gerät zugewiesen wird.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Geräte zuweisen auf Seite 182

Überblick über Geräte anzeigen

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

Um einen Überblick über ein Gerät zu erhalten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Geräte > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Überblick über das Gerät**.

Servicevereinbarungen an Geräte zuweisen und Calls erfassen

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

Über das Helpdeskmodul erfassen Sie Servicevereinbarungen und Calls für ein Gerät. Ausführliche Informationen zum Helpdesk finden Sie im *One Identity Manager Anwenderhandbuch für das Helpdeskmodul*.

Um Helpdeskdaten für ein Gerät zu erfassen

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Geräte > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Servicevereinbarungen zuweisen**, um dem Gerät die gültigen Servicevereinbarungen zuzuweisen.

   Die Servicevereinbarungen werden bei der Ermittlung von Lösungszeiten und Reaktionszeiten im Falle eines Helpdeskcalls zu diesem Gerät berücksichtigt.
4. Wählen Sie die Aufgabe **Calls anzeigen**, um die Calls anzuzeigen, die für ein Gerät erfasst wurden.
5. Wählen Sie die Aufgabe **Neuer Call**, um einen neuen Call zu erfassen.
6. Speichern Sie die Änderungen.

Arbeitsplätze erstellen und bearbeiten

Arbeitsplätze dienen der Zuordnung von verschiedenen Geräten zu einer Arbeitsstation oder einem Server. Über die Einordnung von Arbeitsplätzen in Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder dynamische Rollen können Sie die Zuweisung von Unternehmensressourcen weitgehend automatisieren.

TIPP: Um beim Erzeugen eines Gerätes für eine Arbeitsstation oder einen Server automatisch einen Arbeitsplatz zu erstellen, aktivieren Sie im Designer den Konfigurationsparameter **Hardware | Workdesk | WorkdeskAuto**.

Um einen Arbeitsplatz erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen.**
2. Wählen Sie in der Ergebnisliste einen Arbeitsplatz und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Arbeitsplätze auf Seite 187
- Standortinformationen für Arbeitsplätze auf Seite 189
- Sonstige Informationen für Arbeitsplätze auf Seite 190
- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 190
- Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen auf Seite 233

Allgemeine Stammdaten für Arbeitsplätze

Erfassen Sie die folgenden allgemeinen Stammdaten zu einem Arbeitsplatz.

Tabelle 53: Allgemeine Stammdaten eines Arbeitsplatzes

Eigenschaft	Beschreibung
Arbeitsplatz	Bezeichnung des Arbeitsplatzes. Ist der Konfigurationsparameter **Hardware | Workdesk | WorkdeskAuto** aktiviert, wird beim

Eigenschaft	Beschreibung
	Einrichten einer Arbeitsstation oder eines Servers automatisch ein gleich bezeichneter Arbeitsplatz angelegt.
Arbeitsplatztyp	Typ des Arbeitsplatzes.
Status	Status des Arbeitsplatzes.
Anzeigename	Anzeigename zur Anzeige in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Primäre Kostenstelle	Kostenstelle, der der Arbeitsplatz primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Arbeitsplatz über diese primären Zuordnungen Unternehmensressourcen erhalten.
Primäre Geschäftsrolle	Geschäftsrolle, der die Person primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Arbeitsplatz über diese primären Zuordnungen Unternehmensressourcen erhalten. HINWEIS: Diese Eigenschaft steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.
Installationsdatum	Datum der Inbetriebnahme.
Arbeitsplatzverantwortlicher	Verantwortliche Person für diesen Arbeitsplatz.
Überprüfung durch	Person, die diesen Arbeitsplatz überprüft hat.
Überprüfungsdatum	Datum der letzten Überprüfung.
Überprüfungsbemerkung	Freitextfeld für zusätzliche Erläuterungen.
Servicetyp	Information über den Service für diesen Arbeitsplatz, zum Beispiel interner oder externer Dienstleister.
Entsprechend Servicevereinbarung eingerichtet	Gibt an, ob der Arbeitsplatz entsprechend der Servicevereinbarungen eingerichtet ist. HINWEIS: Diese Eigenschaft steht zur Verfügung, wenn das Helpdeskmodul vorhanden ist.
Keine Vererbung	Gibt an, ob der Arbeitsplatz Unternehmensressourcen über Rollen erbt. Ist die Option aktiviert, wird die Vererbung verhindert. Direkte Zuweisungen bleiben bestehen.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Arbeitsplatztypen erstellen und bearbeiten auf Seite 176
- Arbeitsplatzstatus erstellen und bearbeiten auf Seite 175
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Vererbung an einzelne Personen, Geräte oder Arbeitsplätze verhindern auf Seite 34

Standortinformationen für Arbeitsplätze

Erfassen Sie die folgenden Informationen zum Standort eines Arbeitsplatzes.

Tabelle 54: Standortinformationen eines Arbeitsplatzes

Eigenschaft	Beschreibung
Primäre Abteilung	Abteilung, der der Arbeitsplatz primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Arbeitsplatz über diese primären Zuordnungen Unternehmensressourcen erhalten.
Primärer Standort	Standort, dem der Arbeitsplatz primär zugeordnet ist. Bei entsprechender Konfiguration des One Identity Manager kann ein Arbeitsplatz über diese primären Zuordnungen Unternehmensressourcen erhalten.
Fax	Faxnummer
Bemerkungen (Fax)	Freitextfeld für zusätzliche Erläuterungen.
Gebäude	Gebäude.
Raum	Raum.
Telefon	Telefonnummer.
Etage	Etage.
Bemerkungen (Raum)	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16

Sonstige Informationen für Arbeitsplätze

Erfassen Sie zusätzliche Gerätevoraussetzungen wie beispielsweise die Notwendigkeit von Disketten oder CD-Laufwerken.

Tabelle 55: Sonstige Stammdaten eines Arbeitsplatzes

Eigenschaft	Beschreibung
Einrichtungsdatum	Datum der Inbetriebnahme.
Ausmusterung	Datum, zu dem der Arbeitsplatz abgeschrieben ist.
Leasingrate	Leasingrate.
Diskettenlaufwerk notwendig	Gibt an, ob an diesem Arbeitsplatz ein Floppylaufwerk benötigt wird.
CD-Laufwerk notwendig	Gibt an, ob an diesem Arbeitsplatz ein CD-Laufwerk benötigt wird.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.

Unternehmensressourcen an Arbeitsplätze zuweisen

Um Unternehmensressourcen zuzuweisen, nutzt der One Identity Manager verschiedene Zuweisungsarten.

- Indirekte Zuweisung

  Bei der indirekten Zuweisung von Unternehmensressourcen werden Personen, Geräte und Arbeitsplätze in Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Anwendungsrollen eingeordnet. Aus der Position innerhalb der Hierarchie, der Vererbungsrichtung (Top-Down, Bottom-Up) und den Unternehmensressourcen, die diesen Rollen zugeordnet sind, berechnet sich die Summe der zugeordneten Unternehmensressourcen für eine Person, ein Gerät oder einen Arbeitsplatz. Bei der indirekten Zuweisung von Unternehmensressourcen wird nochmals zwischen der primären Zuweisung und der sekundären Zuweisung unterschieden.
- Direkte Zuweisung

  Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Person, einem Gerät oder einem Arbeitsplatz. Durch die direkte Zuweisung von Unternehmensressourcen kann ohne weiteren Aufwand auf Sonderanforderungen reagiert werden.
- Zuweisung über dynamische Rollen

Die Zuweisung über dynamische Rollen ist ein Spezialfall der indirekten Zuweisung. Dynamische Rollen werden eingesetzt, um Rollenmitgliedschaften dynamisch festzulegen. Dabei werden Personen, Geräte oder Arbeitsplätze nicht fest an eine Rolle zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen. Welche Personen, Geräte oder Arbeitsplätze diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Personen einer Abteilung zugewiesen werden; verlässt eine Person diese Abteilung, verliert sie sofort die zugewiesenen Unternehmensressourcen.

- Zuweisung über Bestellungen

  Die Zuweisung über IT Shop Bestellungen ist ein Spezialfall der indirekten Zuweisung. Damit Unternehmensressourcen über IT Shop Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Unternehmensressourcen, die als Produkte diesem Shop zugeordnet sind, können von den Kunden bestellt werden. Bestellte Unternehmensressourcen werden nach erfolgreicher Genehmigung den Personen zugewiesen. Neben den Unternehmensressourcen können über den IT Shop auch Rollenmitgliedschaften bestellt werden.

  Ausführliche Informationen zu Bestellungen für Arbeitsplätze finden Sie im *One Identity Manager Administrationshandbuch für IT Shop* und im *One Identity Manager Web Portal Anwenderhandbuch*.

In der nachfolgenden Tabelle sind die möglichen Zuweisungen von Unternehmensressourcen an Arbeitsplätze dargestellt.

HINWEIS: Die Unternehmensressourcen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 56: Mögliche Zuweisungen von Unternehmensressourcen an Arbeitsplätze

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkungen
Systemrollen	+	+	
Software	+	+	
Active Directory Gruppen	-	+	Alle Active Directory Computer, welche das Gerät des Arbeitsplatzes referenzieren, werden in die Active Directory Gruppen aufgenommen.
LDAP Gruppen	-	+	Alle LDAP Computer, welche das Gerät des Arbeitsplatzes referenzieren, werden in die LDAP Gruppen aufgenommen.

Detaillierte Informationen zum Thema

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 26
- Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 192
- Arbeitsplätze an Geschäftsrollen zuweisen
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88
- Dynamische Rollen auf Seite 37

Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie den Arbeitsplatz an Abteilungen, Kostenstellen und Standorte zu, damit der Arbeitsplatz über diese Organisationen seine Unternehmensressourcen erhält. Um Unternehmensressourcen an Abteilungen, Kostenstellen oder Standorte zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Organisationen.

Um einen Arbeitsplatz an Abteilungen, Kostenstellen und Standorte zuzuweisen (sekundäre Zuweisung; Standardverfahren)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
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 einen Arbeitsplatz an Abteilungen, Kostenstellen oder Standorte zuzuweisen (primäre Zuweisung)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Passen Sie die folgenden Stammdaten an.
   - **Primäre Abteilung**: Abteilung, der der Arbeitsplatz zugewiesen wird.
   - **Primäre Kostenstelle**: Kostenstelle, der der Arbeitsplatz zugewiesen wird.
   - **Primärer Standort**: Standort, dem der Arbeitsplatz zugewiesen wird.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 190
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 88
- Dynamische Rollen auf Seite 37
- Geräte an Geschäftsrollen zuweisen auf Seite 185
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 87

Arbeitsplätze an Geschäftsrollen zuweisen

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

Weisen Sie den Arbeitsplatz an Geschäftsrollen zu, damit der Arbeitsplatz über diese Geschäftsrollen ihre Unternehmensressourcen erhält. Um Unternehmensressourcen an Geschäftsrollen zuzuweisen, nutzen Sie die entsprechenden Aufgaben an den Geschäftsrollen. Ausführliche Informationen zum Arbeiten mit Geschäftsrollen finden Sie im *One Identity Manager Administrationshandbuch für Geschäftsrollen*.

Um einen Arbeitsplatz an Geschäftsrollen zuzuweisen (sekundäre Zuweisung; Standardverfahren)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um einen Arbeitsplatz an Geschäftsrollen zuzuweisen (primäre Zuweisung)

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen.**
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie in der Auswahlliste **Primäre Geschäftsrolle** die Geschäftsrolle, der der Arbeitsplatz zugewiesen wird.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 190

Software direkt an Arbeitsplätze zuweisen

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

Software kann direkt oder indirekt an Arbeitsplätze zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Arbeitsplätze und der Software in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Arbeitsplatz die Software direkt zuweisen.

Um einem Arbeitsplatz Software zuzuweisen

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Software zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Software zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 192
- Arbeitsplätze an Geschäftsrollen zuweisen auf Seite 193

Systemrollen direkt an Arbeitsplätze zuweisen

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

Systemrollen können direkt oder indirekt an Arbeitsplätze zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Arbeitsplätze und der Systemrollen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen. Ausführliche Informationen zum Arbeiten mit Systemrollen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Arbeitsplatz die Systemrollen direkt zuweisen.

Um einem Arbeitsplatz Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**, um Systemrollen direkt an den Arbeitsplatz zuzuweisen.

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

- Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 192
- Arbeitsplätze an Geschäftsrollen zuweisen auf Seite 193

Überblick über Arbeitsplätze anzeigen

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

Um einen Überblick über einen Arbeitsplatz zu erhalten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Überblick über den Arbeitsplatz**.

Geräte an Arbeitsplätze zuweisen

Nutzen Sie die Aufgabe, um einen Arbeitsplatz an mehrere Geräte, wie beispielsweise Arbeitstation, Server, Drucker, Monitor oder sonstige Peripheriegeräte, zuzuweisen. Sie können den Arbeitsplatz auch über die Stammdaten eines Gerätes zuordnen.

Um Geräte an einen Arbeitsplatz zuzuweisen

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Geräte zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geräte zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Gerät und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Geräte auf Seite 178

Arbeitsplätze an Personen zuweisen

Nutzen Sie die Aufgabe, um einen Arbeitsplatz an mehrere Personen zuzuweisen. Sie können den Arbeitsplatz auch über die Stammdaten einer Person zuordnen.

Um einen Arbeitsplatz an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **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

- Allgemeine Personenstammdaten auf Seite 128

Calls für Arbeitsplätze erfassen

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

Über das Helpdeskmodul erfassen Sie Servicevereinbarungen und Calls für einen Arbeitsplatz. Ausführliche Informationen zum Helpdesk finden Sie im *One Identity Manager Anwenderhandbuch für das Helpdeskmodul*.

Um Helpdeskdaten für einen Arbeitsplatz zu erfassen

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze > Arbeitsplätze > Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Calls anzeigen**, um die Calls anzuzeigen, die für einen Arbeitsplatz erfasst wurden.
4. Wählen Sie die Aufgabe **Neuer Call**, um einen neuen Call zu erfassen.
5. Speichern Sie die Änderungen.

Anlageinformationen für Geräte

Der One Identity Manager bietet die Möglichkeit Angaben zu Anlagen sowie kaufmännische Daten im Rahmen des Bestandsmanagements zu verwalten. Hierzu gehören weiterhin Informationen über Partnerfirmen, Eigentumsverhältnisse (Leasing, Miete, Kauf) und die zugehörigen Vertragsinformationen über Kosten und Zeiträume. Für das Anlagenbestandsmanagement können Daten aus anderen Systemen in den One Identity Manager übernommen werden. So kann beispielsweise eine Datei, die aus der Anlagenbuchhaltung von SAP R/3 gewonnen wurde, als Datenquelle fungieren.

Um diese Funktion zu nutzen

- Aktivieren Sie im Designer den Konfigurationsparameter **Hardware | AssetAccounting** und kompilieren Sie die Datenbank.

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

Detaillierte Informationen zum Thema

- Anlageklassen für Geräte erstellen und bearbeiten auf Seite 199
- Anlagetypen für Geräte erstellen und bearbeiten auf Seite 199
- Basisdaten für die Geräteverwaltung auf Seite 170
- Investitionen und Investitionsvorhaben für Geräte erfassen auf Seite 200
- Anlageinformationen für Geräte bearbeiten auf Seite 201
- Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen auf Seite 233

Anlageklassen für Geräte erstellen und bearbeiten

Erfassen Sie die Anlageklassen für die Anlageinformationen zu einem Gerät.

Um eine Anlageklasse zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Anlageklassen**.
2. Wählen Sie in der Ergebnisliste eine Anlageklasse und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Erfassen Sie die folgenden Stammdaten für eine Anlageklasse.

Tabelle 57: Stammdaten einer Anlageklasse

Eigenschaft	Beschreibung
Anlageklasse	Bezeichnung der Anlageklasse.
Anzeigename	Bezeichnung zur Anzeige in den One Identity Manager-Werkzeugen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Anlagetypen für Geräte erstellen und bearbeiten

Erfassen Sie die Anlagetypen für die Anlageinformationen zu einem Gerät.

Um einen Anlagetyp zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Basisdaten zur Konfiguration > Anlagetypen**.
2. Wählen Sie in der Ergebnisliste einen Anlagetyp und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die Bezeichnung des Anlagetyps und eine Beschreibung zur zusätzlichen

Erläuterung.

4. Speichern Sie die Änderungen.

Investitionen und Investitionsvorhaben für Geräte erfassen

Erfassen Sie Angaben zu Investitionen und Investitionsvorhaben und weisen Sie diese an die Geräte zu.

Um eine Investition zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Investitionen**.
2. Wählen Sie in der Ergebnisliste eine Investition und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die folgenden Stammdaten.

   Tabelle 58: Stammdaten für Investitionen

Eigenschaft	Beschreibung
Investition	Bezeichnung des Investitionsvorhabens.
Datum	Datum der Investition.
Investitionsverantwortlicher	Person, die für diese Investition verantwortlich ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Geräte auf Seite 178

Anlageinformationen für Geräte bearbeiten

Um die Anlageinformationen für ein Gerät zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geräte & Arbeitsplätze > Geräte > <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Kaufmännische Daten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für die Anlageinformationen.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten für die Anlageinformationen für Geräte auf Seite 201
- Kaufmännische Daten für Geräte auf Seite 202

Stammdaten für die Anlageinformationen für Geräte

Erfassen Sie die folgenden Stammdaten für die Anlageinformationen eines Gerätes.

HINWEIS: Die Angabe der Preise erfolgt standardmäßig mit 2 Nachkommastellen. Die Anzahl der anzugebenden Kommastellen kann im Designer unternehmensspezifisch angepasst werden. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Tabelle 59: Anlageinformationen eines Gerätes

Eigenschaft	Beschreibung
Anlagegut Nummer	Nummer des Anlagegutes in der Anlagenbuchhaltung.
Anlagegut	Anlagegut.
Anlageklasse	Anlageklasse.
Anlagetyp	Anlagetyp.
Gerätestatus	Status des Gerätes.
Aktivierung	Datum der Anlagenaktivierung beziehungsweise Beginn des Mietzeitraums.
Deaktivierung	Datum der Anlagendeaktivierung beziehungsweise Ende des Mietzeitraums.
Neuwert	Neuwert des Gerätes.

Eigenschaft	Beschreibung
Restbuchwert	Restbuchwert des Gerätes.
Firmeneigentum	Gibt an, ob es sich um Eigentum der Firma handelt.
Leasing	Gibt an, ob das Gerät geleast wurde.
Rechnungsnummer	Rechnungsnummer der Anschaffung.
PSP Zeichenkette	Anlage PSP als Zeichenkette.
Letzte Inventur	Datum der letzten Inventur.
Primäre Kostenstelle	Kostenstelle. Bei entsprechender Konfiguration des One Identity Manager kann ein Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten.
Seriennummer	Seriennummer des Gerätes.
Lieferbemerkung	Freitextfeld für zusätzliche Erläuterungen.
Inventurbemerkung	Freitextfeld für zusätzliche Erläuterungen.
Primäre Geschäftsrolle	Geschäftsrolle. Bei entsprechender Konfiguration des One Identity Manager kann ein Arbeitsplatz über diese primären Zuordnungen Unternehmensressourcen erhalten. HINWEIS: Diese Eigenschaft steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.
Primärer Standort	Standort. Bei entsprechender Konfiguration des One Identity Manager kann ein Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten.
Primäre Abteilung	Abteilung. Bei entsprechender Konfiguration des One Identity Manager kann ein Gerät über diese primären Zuordnungen Unternehmensressourcen erhalten.

Verwandte Themen

- Anlageklassen für Geräte erstellen und bearbeiten auf Seite 199
- Anlagetypen für Geräte erstellen und bearbeiten auf Seite 199
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16

Kaufmännische Daten für Geräte

Erfassen Sie die folgenden kaufmännischen Informationen zu einem Gerät.

HINWEIS: Die Angabe der Preise erfolgt standardmäßig mit 2 Nachkommastellen. Die Anzahl der anzugebenden Kommastellen kann im Designer unternehmensspezifisch angepasst werden. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Tabelle 60: Kaufmännische Daten eines Gerätes

Eigenschaft	Beschreibung
Anschaffungsdatum	Datum des Kaufs.
Lieferdatum	Datum der Lieferung.
Lieferscheinnummer	Lieferscheinnummer.
Beleg	Beleg. Ausführliche Informationen zu Belegen finden Sie im *One Identity Manager Administrationshandbuch für die Leistungs-abrechnung*.
Garantie	Ablaufdatum der Garantie.
Garantienummer	Garantienummer.
Einrichtungsdatum	Datum der Inbetriebnahme.
Eigentümer	Leasingfirma.
Lieferant	Lieferantenfirma.
Hersteller	Herstellerfirma.
Einkaufspreis	Einkaufspreis.
Interner Preis	Interner Preis.
Verkaufspreis	Verkaufspreis.
Währung	Währungseinheit.
Inventurvermerk	Freitextfeld für zusätzliche Erläuterungen.
Ausmusterung	Datum, zu dem das Gerät abgeschrieben ist.
Investition	Investition oder Investitonsvorhaben.
Leasingrate	Leasingrate.
Interner Verrechnungspreis	Interner Verrechnungspreis.
Abschreibungsmonat	Abschreibungsdauer in Monaten.

Verwandte Themen

- Partnerfirmen erstellen und bearbeiten auf Seite 173
- Investitionen und Investitionsvorhaben für Geräte erfassen auf Seite 200

6

Ressourcen verwalten

Der One Identity Manager bietet neben der Verwaltung von IT-Ressourcen auch die Möglichkeit Nicht-IT-Ressourcen abzubilden, die zur Herstellung der Arbeitsfähigkeit von Personen notwendig sind, wie beispielsweise Mobiltelefone, Schreibtische, Dienstwagen oder Schlüssel. Ressourcen können im One Identity Manager den Personen direkt oder über die Einordnung in hierarchische Rollen zugewiesen werden. Ebenso sind Ressourcen über den IT Shop bestellbar.

Ressourcen werden nach funktionalen Gesichtspunkten unterteilt.

Tabelle 61: Ressourcenarten

Art	Beschreibung	Tabelle
Ressourcen	Ressourcen, die eine Person (ein Arbeitsplatz, ein Gerät) genau ein Mal besitzen kann. Die Ressourcen können genau ein Mal im IT Shop bestellt werden. Nach Genehmigung werden die Ressourcen an die Personen zugewiesen. Sie bleiben so lange zugewiesen, bis sie abbestellt werden. Danach können Sie erneut bestellt werden. Beispiele: Telefon, Dienstwagen	QERResource
Mehrfach bestellbare Ressourcen	Ressourcen, die eine Person mehrfach im IT Shop bestellen kann. Nach Genehmigung werden die Bestellungen automatisch abbestellt. Die Ressourcen werden nicht explizit an die Personen zugewiesen. Beispiele: Ressource zur Anforderung von Remote-Desktop Sitzungen für Assets in einem PAM System; Verbrauchsmaterialen, wie Stifte, Druckerpapier	QERReuse
Mehrfach zu-/ abbestellbare Ressourcen	Ressourcen, die eine Person mehrfach im IT Shop bestellen kann, die jedoch explizit zurück-gegeben werden müssen, wenn sie nicht mehr	QERReuseUS

Art	Beschreibung	Tabelle
	benötigt werden. Nach Genehmigung werden die Ressourcen an die Personen zugewiesen. Sie bleiben so lange zugewiesen, bis sie abbestellt werden. Beispiele: Drucker, Monitor	
Zuweisungsressourcen	Zuweisungsressourcen sind spezielle Ressourcen, über die im IT Shop beliebige Zuweisungen zu hierarchischen Rollen oder die Delegierung von Verantwortlichkeiten bestellt werden. Ausführliche Informationen über Zuweisungsressourcen erhalten Sie im *One Identity Manager Administrationshandbuch für IT Shop*.	`QERAssign`

Detaillierte Informationen zum Thema

- Ressourcen erstellen und bearbeiten auf Seite 207
- Ressourcen an Personen zuweisen auf Seite 209
- Mehrfach bestellbare Ressourcen erstellen und bearbeiten auf Seite 214
- Mehrfach bestellbare Ressourcen an Personen zuweisen auf Seite 216
- Berichte über Ressourcen auf Seite 219

One Identity Manager Benutzer für die Verwaltung von Ressourcen

In die Verwaltung von Ressourcen sind folgende Benutzer eingebunden.

Tabelle 62: Benutzer

Benutzer	Aufgaben
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten Ressourcen und weisen diese an IT Shop-Strukturen zu.
One Identity Manager	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in

Benutzer	Aufgaben
Administratoren	Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Basisdaten für Ressourcen

Für die Verwaltung von Ressourcen werden die folgenden Basisdaten benötigt.

- Ressourcentypen

  Ressourcentypen können zur Gruppierung von Ressourcen genutzt werden.
- Zusatzeigenschaften

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

Detaillierte Informationen zum Thema

- Ressourcentypen auf Seite 206
- Zusatzeigenschaften erstellen und bearbeiten auf Seite 222

Ressourcentypen

Ressourcentypen können zur Gruppierung von Ressourcen genutzt werden.

Um Ressourcentypen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Ressourcentypen**.
2. Wählen Sie in der Ergebnisliste einen Ressourcentyp und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   – ODER –

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie eine Bezeichnung und eine Beschreibung für den Ressourcentyp.
4. Speichern Sie die Änderungen.

Ressourcen erstellen und bearbeiten

Um Ressourcen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste eine Ressource und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Stammdaten für Ressourcen auf Seite 207
- Ressourcen an Personen zuweisen auf Seite 209

Stammdaten für Ressourcen

Für eine Ressource erfassen Sie folgende allgemeine Stammdaten.

Tabelle 63: Stammdaten einer Ressource

Eigenschaft	Beschreibung
Ressource	Bezeichnung der Ressource.
Ressourcentyp	Ressourcentyp zur Gruppierung von Ressourcen.

Eigenschaft	Beschreibung
Leistungsposition	Leistungsposition, über welche die Ressource im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
Vorausgesetzte Ressource	Definieren Sie Abhängigkeiten zwischen Ressourcen. Wenn die Ressource bestellt oder zugeordnet wird, wird die vorausgesetzte Ressource automatisch zugeordnet.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Ressource an Personen. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
IT Shop	Gibt an, ob die Ressource über den IT Shop bestellbar ist. Die Ressource kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Ressource kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Verwendung nur im IT Shop	Gibt an, ob die Ressource über den IT Shop bestellbar ist. Die Ressource kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Ressource an Rollen außerhalb des IT Shop ist nicht zulässig. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Keine Vererbung bei Sicherheitsgefährdung	Ressourcen, die mit dieser Option gekennzeichnet sind, werden nicht an Personen vererbt, die als sicherheitsgefährdend eingestuft sind.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatische Zuweisung an Personen	Gibt an, ob die Ressource automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Ressource an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Ressource. Um die automatische Zuweisung der Ressource an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Ressource nicht neu an Personen

Eigenschaft	Beschreibung
	zugewiesen. Bestehende Zuweisungen der Ressource bleiben jedoch erhalten.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Ressourcentypen auf Seite 206
- Allgemeine Personenstammdaten auf Seite 128
- Berechnung der Zuweisungen auf Seite 23

Ressourcen an Personen zuweisen

Ressourcen können direkt, indirekt oder über IT Shop-Bestellungen an Personen zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Ressourcen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Ressourcen, die einer Person zugewiesen ist. Damit Ressourcen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Ressourcen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Ressourcen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Voraussetzung für die indirekte Zuweisung von Ressourcen an Personen

- An den Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Personen und Ressourcen erlaubt.

Detaillierte Informationen zum Thema

- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen an Rollen erlauben auf Seite 31
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16

Ressourcen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie eine Ressource an Abteilungen, Kostenstellen oder Standorte zu, damit die Ressource über diese Organisationen an Personen vererbt wird.

Um eine Ressource an Abteilungen, Kostenstellen oder Standorte zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
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

- Abteilungen, Kostenstellen und Standorte auf Seite 56
- Grundlagen zur Abbildung von Unternehmensstrukturen im One Identity Manager auf Seite 10

Ressourcen an Geschäftsrollen zuweisen

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

Weisen Sie eine Ressource an Geschäftsrollen zu, damit die Ressource über diese Geschäftsrollen an Personen vererbt wird. Ausführliche Informationen zum Arbeiten mit Geschäftsrollen finden Sie im *One Identity Manager Administrationshandbuch für Geschäftsrollen*.

Um eine Ressource an Geschäftsrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.

3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Ressourcen direkt an Personen zuweisen

Ressourcen können direkt oder indirekt an Personen zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Personen und der Ressourcen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie Ressourcen direkt an Personen zuweisen.

Um eine Ressource direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
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

- Personen verwalten auf Seite 99
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 16

Ressourcen in den IT Shop aufnehmen

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

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

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

Um eine Ressource in den IT Shop aufzunehmen

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

Um eine Ressource aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Ressource aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Ressource aus allen Regalen des IT Shops zu entfernen

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

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

Verwandte Themen

- Stammdaten für Ressourcen auf Seite 207

Ressourcen in Systemrollen aufnehmen

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

Eine Ressource kann in verschiedene Systemrollen aufgenommen werden. Eine Systemrolle, in der ausschließlich Ressourcen zusammengefasst sind, können mit dem Systemrollentyp **Ressourcenpaket** gekennzeichnet werden. Ressourcen können auch in Systemrollen aufgenommen werden, die keine Ressourcenpakete sind. Wenn Sie eine Systemrolle an Personen zuweisen, wird die Ressource diesen Personen zugewiesen.

Ausführliche Informationen zum Arbeiten mit Systemrollen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen.*

HINWEIS: Ressourcen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist.

Um eine Ressource an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste eine Ressource.
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.

Überblick über Ressourcen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Ressource. Dazu zählt die Zugehörigkeit der Ressource zu hierarchischen Rollen und IT Shop-Strukturen.

Um einen Überblick über eine Ressource zu erhalten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
3. Wählen Sie die Aufgabe **Überblick über die Ressource**.

Zusatzeigenschaften an Ressourcen 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 Ressource festzulegen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
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.

Detaillierte Informationen zum Thema

- Zusatzeigenschaften erstellen und bearbeiten auf Seite 222

Mehrfach bestellbare Ressourcen erstellen und bearbeiten

Mehrfach bestellbare Ressourcen können nur bearbeitet werden, wenn der Konfigurationsparameter **QER | ITShop** aktiviert ist.

- Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

Um mehrfach bestellbare Ressourcen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach bestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste eine Ressource und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .

3. Bearbeiten Sie die Stammdaten der mehrfach bestellbaren Ressource.
4. Speichern Sie die Änderungen.

Um mehrfach zu-/abbestellbare Ressourcen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste eine Ressource und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der mehrfach zu-/abbestellbaren Ressource.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten für mehrfach bestellbare Ressourcen auf Seite 215
- Mehrfach bestellbare Ressourcen an Personen zuweisen auf Seite 216
- Mehrfach bestellbare Ressourcen in den IT Shop aufnehmen auf Seite 217

Stammdaten für mehrfach bestellbare Ressourcen

Für eine mehrfach bestellbare Ressource erfassen Sie folgende allgemeine Stammdaten.

Tabelle 64: Stammdaten einer mehrfach bestellbaren Ressource

Eigenschaft	Beschreibung
Mehrfach bestellbare Ressource	Bezeichnung der Ressource.
Mehrfach zu-/abbestellbare Ressource	
Ressourcentyp	Ressourcentyp zur Gruppierung von Ressourcen.
Leistungsposition	Leistungsposition, über welche die Ressource im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Ressource an Personen. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter

Eigenschaft	Beschreibung
	QER | CalculateRiskIndex aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
IT Shop	Gibt an, ob die Ressource über den IT Shop bestellbar ist. Die Ressource kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Ressource kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden. Diese Option kann nicht deaktiviert werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Verwendung nur im IT Shop	Gibt an, ob die Ressource über den IT Shop bestellbar ist. Die Ressource kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Ressource an Rollen außerhalb des IT Shop ist nicht zulässig. Diese Option kann nicht deaktiviert werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Ressourcentypen auf Seite 206

Mehrfach bestellbare Ressourcen an Personen zuweisen

Mehrfach bestellbare Ressourcen können über IT Shop-Bestellungen an Personen zugewiesen werden. Dafür werden Personen als Kunden in einen Shop aufgenommen. Alle Ressourcen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Detaillierte Informationen zum Thema

- Mehrfach bestellbare Ressourcen in den IT Shop aufnehmen auf Seite 217
- Zuweisung von Unternehmensressourcen über IT Shop Bestellungen auf Seite 20

Mehrfach bestellbare Ressourcen in den IT Shop aufnehmen

Mit der Zuweisung einer mehrfach bestellbaren Ressource an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Um mehrfach bestellbare Ressourcen einzurichten und als Produkte in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach bestellbare Ressourcen für IT Shop**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Ressource.
4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** ein Regal zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Regal und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um mehrfach zu-/abbestellbare Ressourcen einzurichten und als Produkte in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Ressource.
4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** ein Regal zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Regal und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Um eine mehrfach bestellbare Ressource aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach bestellbare Ressourcen für IT Shop**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste die Ressource.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

Überblick über mehrfach bestellbare Ressourcen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer mehrfach bestellbaren Ressource. Dazu zählt die Zugehörigkeit der Ressource zu IT Shop-Strukturen.

Um einen Überblick über eine mehrfach bestellbare Ressource zu erhalten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach bestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste die Ressource.
3. Wählen Sie die Aufgabe **Überblick über die mehrfach bestellbare Ressource**.

Um einen Überblick über eine mehrfach zu-/abbestellbare Ressource zu erhalten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste die Ressource.

3. Wählen Sie die Aufgabe **Überblick über die mehrfach zu-/abbestellbare Ressource**.

Berichte über Ressourcen

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 Ressourcen stehen folgende Berichte zur Verfügung.

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

Tabelle 65: Berichte über Ressourcen

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die die ausgewählte Ressource besitzen.

Verwandte Themen

- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 158

Zusatzeigenschaften einrichten

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche. Zusatzeigenschaften können an Unternehmensressourcen, hierarchische Rollen und Personen zugewiesen werden. Sie können beispielsweise in den Regelbedingungen von Complianceregeln genutzt werden.

Um Zusatzeigenschaften abzubilden

1. Richten Sie eine Eigenschaftengruppe ein, unter der die Zusatzeigenschaften zusammengefasst werden.
2. Unterhalb einer Eigenschaftengruppe richten Sie die Zusatzeigenschaften ein.
3. Weisen Sie die Zusatzeigenschaften an die Objekte zu.

   Es können beliebig viele Objekte der unterschiedlichen Objekttypen an eine Zusatzeigenschaft zugewiesen werden.

Detaillierte Informationen zum Thema

- Eigenschaftengruppen für Zusatzeigenschaften erstellen auf Seite 221
- Zusatzeigenschaften erstellen und bearbeiten auf Seite 222

One Identity Manager Benutzer für die Verwaltung von Zusatzeigenschaften

In die Verwaltung von Zusatzeigenschaften sind folgende Benutzer eingebunden.

Tabelle 66: Benutzer

Benutzer	Aufgaben
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein.

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Erstellen Zusatzeigenschaften für beliebige Unternehmensressourcen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Eigenschaftengruppen für Zusatzeigenschaften erstellen

Eigenschaftengruppen werden genutzt, um Zusatzeigenschaften zu gruppieren. Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein.

Um eine Eigenschaftengruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie eine Bezeichnung und eine Beschreibung für die Eigenschaftengruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Zusatzeigenschaften an Eigenschaftengruppen zuweisen auf Seite 223
- Stammdaten für Zusatzeigenschaften auf Seite 222
- Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen auf Seite 224

Zusatzeigenschaften erstellen und bearbeiten

Um eine Zusatzeigenschaft zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste eine Zusatzeigenschaft. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Stammdaten für Zusatzeigenschaften auf Seite 222
- Bereichsgrenzen für Zusatzeigenschaften festlegen auf Seite 225

Stammdaten für Zusatzeigenschaften

Für eine Zusatzeigenschaft erfassen Sie die folgenden Stammdaten.

Tabelle 67: Stammdaten einer Zusatzeigenschaft

Eigenschaft	Beschreibung
Name der Zusatzeigenschaft	Bezeichnung der Zusatzeigenschaft.
Eigenschaftengruppe	Die Eigenschaftengruppen dienen zur Strukturierung der Zusatzeigenschaften. Zu einer Zusatzeigenschaft können Sie über das Stammdatenformular eine Eigenschaftengruppe zuweisen. Die Zusatzeigenschaften werden in der

Eigenschaft	Beschreibung
	Navigationsansicht nach dieser Eigenschaftengruppe gruppiert. Sollte die Zuordnung einer Zusatzeigenschaft zu mehreren Eigenschaftengruppen notwendig sein, so können Sie zusätzliche Eigenschaftengruppen zuweisen.
Untere Bereichsgrenze	Untere Bereichsgrenze zur weiteren Unterteilung.
Obere Bereichsgrenze	Obere Bereichsgrenze zur weiteren Unterteilung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Bereichsgrenzen für Zusatzeigenschaften festlegen auf Seite 225
- Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen
- Zusatzeigenschaften an Eigenschaftengruppen zuweisen

Zusatzeigenschaften an Eigenschaftengruppen zuweisen

Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein.

Sollen einer Eigenschaftengruppe weitere Zusatzeigenschaften zugewiesen werden, verwenden Sie die Aufgabe **Zusatzeigenschaften zuweisen**.

Um Zusatzeigenschaften an eine Eigenschaftengruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften**.
2. Wählen Sie in der Ergebnisliste eine Eigenschaftengruppe.
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.

Verwandte Themen

- Stammdaten für Zusatzeigenschaften auf Seite 222
- Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen auf Seite 224

Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen

Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein. Sollte die Zuordnung einer Zusatzeigenschaft zu mehreren Eigenschaftengruppen notwendig sein, so können Sie über die Aufgabe **Eigenschaftengruppen zuweisen** zusätzliche Eigenschaftengruppen zuweisen.

Um eine Zusatzeigenschaft an Eigenschaftengruppen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste eine Zusatzeigenschaft.
3. Wählen Sie die Aufgabe **Eigenschaftengruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigenschaftengruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Eigenschaftengruppe und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Zusatzeigenschaften auf Seite 222
- Zusatzeigenschaften an Eigenschaftengruppen zuweisen auf Seite 223

Bereichsgrenzen für Zusatzeigenschaften festlegen

Über Bereichsgrenzen können Sie innerhalb der Zusatzeigenschaften eine weitere Unterteilung vornehmen. Die Angabe von Bereichsgrenzen für Zusatzeigenschaften ist nicht zwingend erforderlich. Wenn Sie eine untere Bereichsgrenze definieren, müssen Sie nicht unbedingt eine obere Bereichsgrenze festlegen. Wenn Sie jedoch eine obere Bereichsgrenze angeben, so müssen Sie auch eine untere Bereichsgrenze festlegen.

Bei der Definition von Bereichsgrenzen beachten Sie Folgendes:

- Grundsätzlich ist jede beliebige Zeichenkette als untere oder obere Bereichsgrenze zulässig.
- Als Platzhalter für beliebig viele (auch Null) Zeichen kann ***** verwendet werden.
- Platzhalter dürfen nur am Ende einer Zeichenkette stehen, beispielsweise AB*. Nicht zulässig ist beispielsweise *AB oder A*B.
- Wenn Sie die untere Bereichsgrenze ohne Platzhalter angeben, dann dürfen Sie auch für die obere Bereichsgrenze keinen Platzhalter verwenden.

Für die Zeichenkettenlänge gibt es folgende Einschränkungen:

- Wenn Sie die untere Bereichsgrenze und die obere Bereichsgrenze ohne Platzhalter eintragen, so müssen beide Zeichenketten gleich lang sein, beispielsweise untere Bereichsgrenze 123/obere Bereichsgrenze 456. Nicht zulässig ist beispielsweise untere Bereichsgrenze 123/obere Bereichsgrenze 45 oder untere Bereichsgrenze 123/obere Bereichsgrenze 4567.
- Wenn Sie in der unteren Bereichsgrenze einen Platzhalter verwenden und in der oberen Bereichsgrenzen keinen Platzhalter nutzen, dann muss die Zeichenkettenlänge der oberen Bereichsgrenze gleich oder größer der Zeichenkettenlänge der unteren Bereichsgrenze sein.
- Wenn Sie in der unteren Bereichsgrenze und in der oberen Bereichsgrenze einen Platzhalter verwenden, so müssen beide Zeichenketten gleich lang sein, beispielsweise untere Bereichsgrenze 123*/obere Bereichsgrenze 456*. Nicht zulässig sind beispielsweise untere Bereichsgrenze 123*/obere Bereichsgrenze 45* oder untere Bereichsgrenze 123*/obere Bereichsgrenze 4567*.

Überblick über Zusatzeigenschaften anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Zusatzeigenschaft. Dazu zählt die Zugehörigkeit der Zusatzeigenschaft zu den verschiedenen Objekten des One Identity Manager.

Um einen Überblick über eine Zusatzeigenschaft zu erhalten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste die Zusatzeigenschaft.
3. Wählen Sie die Aufgabe **Überblick über die Zusatzeigenschaft**.

Um einen Überblick über eine Eigenschaftengruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften**.
2. Wählen Sie in der Ergebnisliste die Eigenschaftengruppe.
3. Wählen Sie die Aufgabe **Überblick über die Eigenschaftengruppe**.

Objekte an Zusatzeigenschaften zuweisen

Zusatzeigenschaften können an Unternehmensressourcen, hierarchische Rollen und Personen zugewiesen werden.

Um eine Zusatzeigenschaft an Objekte zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste eine Zusatzeigenschaft.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** den gewünschten Objekttyp.

   Es werden die zum Objekttyp gehörigen Objekte auf dem Formular angezeigt.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Objekte zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Objekt und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Anhang A

Konfigurationsparameter für die Verwaltung von Abteilungen, Kostenstellen und Standorten

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

Tabelle 68: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | Structures	Steuert, ob hierarchische Rollen unterstützt werden.
QER | Structures | DynamicGroupCheck	Steuert die Erzeugung von Berechnungsaufträgen für dynamische Rollen. Ist der Konfigurationsparameter deaktiviert, sind auch die untergeordneten Konfigurationsparameter nicht wirksam.
QER | Structures | DynamicGroupCheck | CalculateImmediatelyPerson	Ist der Konfigurationsparameter aktiviert, wird bei Änderungen an Personen oder Personen-nahen Objekten sofort ein Berechnungsauftrag für den DBQueue Prozessor eingestellt. Ist der Parameter nicht aktiviert, werden die Berechnungsaufträge beim nächsten geplanten Lauf des Zeitplans eingestellt.
QER | Structures | DynamicGroupCheck | CalculateImmediatelyHardware	Ist der Konfigurationsparameter aktiviert, wird bei Änderungen an Geräten oder Geräte-nahen Objekten sofort ein Berechnungsauftrag für den DBQueue Prozessor eingestellt. Ist der Parameter nicht aktiviert, werden die Berechnungsaufträge beim nächsten Lauf des Zeitplans eingestellt.
QER | Structures | DynamicGroupCheck | CalculateImmediatelyWorkdesk	Ist der Konfigurationsparameter aktiviert, wird bei Änderungen an Arbeitsplätzen oder Arbeitsplatz-nahen Objekten sofort ein Berechnungsauftrag für den DBQueue Prozessor eingestellt. Ist der Parameter nicht aktiviert, werden die Berechnungsaufträge beim nächsten Lauf des Zeitplans eingestellt.

Konfigurationsparameter	Beschreibung
QER | Structures | ExcludeStructures	Präprozessorrelevanter Konfigurationsparameter zur Definition der Wirksamkeit von Rollenmitgliedschaften. Ist der Parameter aktiviert, können sich ausschließende Rollen definiert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | Structures | Inherite | Person	Legt fest, ob Personen über primäre Zuweisung erben.
QER | Structures | Inherite | Person | FromDepartment	Legt fest, ob Personen die Zuordnungen von ihrer primären Abteilung (`Person.UID_Department`) erben.
QER | Structures | Inherite | Person | FromLocality	Legt fest, ob Personen die Zuordnungen von ihrem primären Standort (`Person.UID_Locality`) erben.
QER | Structures | Inherite | Person | FromProfitCenter	Legt fest, ob Personen die Zuordnungen von ihrer primären Kostenstelle (`Person.UID_ProfitCenter`) erben.
QER | Structures | Inherite | Hardware	Legt fest, ob Geräte über primäre Zuweisung erben.
QER | Structures | Inherite | Hardware | FromDepartment	Legt fest, ob Geräte die Zuordnungen von ihrer primären Abteilung (`Hardware.UID_Department`) erben.
QER | Structures | Inherite | Hardware | FromLocality	Legt fest, ob Geräte die Zuordnungen von ihrem primären Standort (`Hardware.UID_Locality`) erben.
QER | Structures | Inherite | Hardware | FromProfitCenter	Legt fest, ob Geräte die Zuordnungen von ihrer primären Kostenstelle (`Hardware.UID_ProfitCenter`) erben.
QER | Structures | Inherite | Workdesk	Legt fest, ob Arbeitsplätze über primäre Zuweisung erben.
QER | Structures | Inherite | Workdesk | FromDepartment	Legt fest, ob Arbeitsplätze die Zuordnungen von ihrer primären Abteilung (`Workdesk.UID_Department`) erben.

Konfigurationsparameter	Beschreibung
QER | Structures | Inherite | Workdesk | FromLocality	Legt fest, ob Arbeitsplätze erben die Zuordnungen von ihrem primären Standort (`Workdesk.UID_Locality`) erben.
QER | Structures | Inherite | Workdesk | FromProfitCenter	Legt fest, ob Arbeitsplätze die Zuordnungen von ihrer primären Kostenstelle (`Workdesk.UID_ProfitCenter`) erben.

Anhang B

Konfigurationsparameter für die Verwaltung von Personen

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

Tabelle 69: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | Person	Ist der Konfigurationsparameter aktiviert, wird die Verwaltung von Personen unterstützt.
QER | Person | AllowLoginWithSecurityIncident	Gibt an, ob sich Personen, die als sicherheitsgefährdend eingestuft sind, am One Identity Manager anmelden dürfen. Ist der Konfigurationsparameter aktiviert, ist die Anmeldung möglich. Ist der Konfigurationsparameter deaktiviert, können sich sicherheitsgefährdende Personen nicht anmelden (Standard).
QER | Person | CentralAccountGlobalUnique	Gibt an, wie das zentrale Benutzerkonto abgebildet wird. Ist der Konfigurationsparameter aktiviert erfolgt die Bildung des zentralen Benutzerkonto einer Person eindeutig bezogen auf die zentralen Benutzerkonten aller Personen und die Benutzerkontennamen aller erlaubten Zielsystemen. Ist der Konfigurationsparameter nicht aktiviert, erfolgt die Bildung nur eindeutig bezogen auf die zentralen Benutzerkonten aller Personen.
QER | Person | DefaultMailDomain	Standardmaildomäne. Der Wert dient zur Bestimmung der Standard-E-Mail-Adresse einer Person.

Konfigurationsparameter	Beschreibung
Person | MasterIdentity | UseMasterForAuthentication	Gibt an, ob zur Anmeldung an One Identity Manager-Werkzeugen über personengebundene Authentifizierungsmodule die Hauptidentität genutzt werden soll. Ist der Parameter aktiviert, wird die Hauptidentität für personengebundene Authentifizierungen genutzt. Ist der Parameter deaktiviert, wird die Subidentität für personengebundene Authentifizierungen genutzt.
QER | Person | PasswordResetAuthenticator | InvalidateUsedQuery	Gibt an, ob die Kennwortfragen, die für eine erfolgreiche Kennwortrücksetzung verwendet wurden, ungültig werden.
QER | Person | PasswordResetAuthenticator | QueryAnswerDefinitions	Anzahl von Kennwortfragen, die eine Person festlegen muss, um ihr Kennwort ändern zu können.
QER | Person | PasswordResetAuthenticator | QueryAnswerRequests	Anzahl von Kennwortfragen, die eine Person beantworten muss, um ihr Kennwort zu ändern.
QER | Person | PasswordResetAuthenticator | PasscodeSplit	Gibt an, ob ein durch den Helpdesk generierter Zugangscode in zwei Bestandteile aufgeteilt wird, einen für den Helpdesk und einen für den Manager der Person.
QER | Person | TemporaryDeactivation	Steuert das Verhalten zwischen Personen und Benutzerkonten bei zeitweiliger Deaktivierung der Personen. Ist der Konfigurationsparameter aktiviert, werden für die Zeit der zeitweiligen Deaktivierung die Benutzerkonten der Person gesperrt. Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der verbundenen Person keinen Einfluss auf die Benutzerkonten.
QER | Person | UseCentralPassword	Gibt an, ob das zentrale Kennwort einer Person in den Benutzerkonten verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
QER | Person | UseCentralPassword | CheckAllPolicies	Gibt an, ob das zentrale Kennwort einer Person gegen alle Kennwortrichtlinien der Zielsysteme geprüft werden soll, in denen die Person Benutzerkonten

Konfigurationsparameter	Beschreibung
	besitzt. Die Prüfung erfolgt nur im Kennwortrücksetzungsportal.
QER | Person | UseCentralPassword | SyncToSystemPassword	Gibt an, ob das zentrale Kennwort der Person auf das Systembenutzerkennwort der Person übernommen wird.
QER | Person | UseCentralPassword | SyncToSystemPassword | UnlockByCentralPassword	Gibt an, ob das Systembenutzerkonto der Person bei der Synchronisation des zentralen Kennworts auch entsperrt wird.
SysConfig	Erlaubt die Konfiguration allgemeiner Einstellungen zum Systemverhalten.
SysConfig | Display	Erlaubt die Konfiguration der Frontendgestaltung.
SysConfig | Display | SourceDetective	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Anzeige der Herkunft von Berechtigungen einer Person. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

Anhang C

Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen

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

Tabelle 70: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
Hardware	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Geräteverwaltung. Ist der Parameter aktiviert, sind die Bestandteile der Geräteverwaltung verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
Hardware | AssetAccounting	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für Daten zur Anlagenbuchhaltung. Ist der Parameter aktiviert, sind die Bestandteile zur Anlagenbuchhaltung verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präpro-

Konfigurationsparameter	Beschreibung
	zessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
Hardware | Display	Legt fest, ob die Anzeige von Geräteeigenschaften konfiguriert werden kann.
Hardware | Display | CustomHardwareType	Legt fest, ob beim Einrichten eines neuen Gerätes mit dem entsprechenden Gerätemodell auf die Stammdaten angepasste Formulare angezeigt werden.
Hardware | Display | CustomHardwareType | MobilePhone	Angabe des Gerätetyps, der ein Mobiltelefone repräsentiert.
Hardware | Display | CustomHardwareType | Monitor	Angabe des Gerätetyps, der einen Monitor repräsentiert.
Hardware | Display | CustomHardwareType | PC	Angabe des Gerätetyps, der einen PC repräsentiert.
Hardware | Display | CustomHardwareType | Printer	Angabe des Gerätetyps, der einen Drucker repräsentiert.
Hardware | Display | CustomHardwareType | Server	Angabe des Gerätetyps, der einen Server repräsentiert.
Hardware | Display | CustomHardwareType | Tablet	Angabe des Gerätetyps, der ein Tablet repräsentiert.
Hardware | Display | DisplayResolutions	Pipe-getrennte Auflistung aller Bildschirmauflösungen, die auf den Stammdatenformularen der Geräte zur Auswahl angeboten werden.
Hardware | Display | MachineWithRPL	Legt fest, ob Angaben zum Remote Boot für Arbeitsstationen und Server bearbeitbar sind.
Hardware | Workdesk	Ist der Konfigurationsparameter aktiviert, wird die Verwaltung von Arbeitsplätzen unterstützt.
Hardware | Workdesk | WorkdeskAuto	Legt fest, ob bei Einrichtung einer Arbeitsstation oder eines Servers automatisch ein zugehöriger Arbeitsplatz erzeugt wird.
Hardware | Workdesk | WorkdeskAutoPerson	Ist der Konfigurationsparameter aktiviert, wird bei Erstellen eines Arbeitsplatzes automatisch eine zugehöriges Personenobjekt erzeugt. Dieses Personenobjekt

Konfigurationsparameter	Beschreibung
	kann für Bestellungen für diesen Arbeitsplatz genutzt werden.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

B

D

E

G

H

I

K

L

M

O

P

R

S

U

V

Z