One Identity Manager 8.1.4

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 - 19. Oktober 2020, 07:35 Uhr
Version - 8.1.4

Inhalt

1

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 Bearbeitungsrechte auf die One Identity Manager Objekte an die One Identity Manager Benutzer zu vergeben. Ausführliche

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

Detaillierte Informationen zum Thema

- Grundlagen für den Aufbau von hierarchischen Rollen auf Seite 10
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14
- Grundlagen zur Berechnung der Vererbung auf Seite 19
- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 23

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 10
- Unterbrechen der Vererbung auf Seite 13

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.

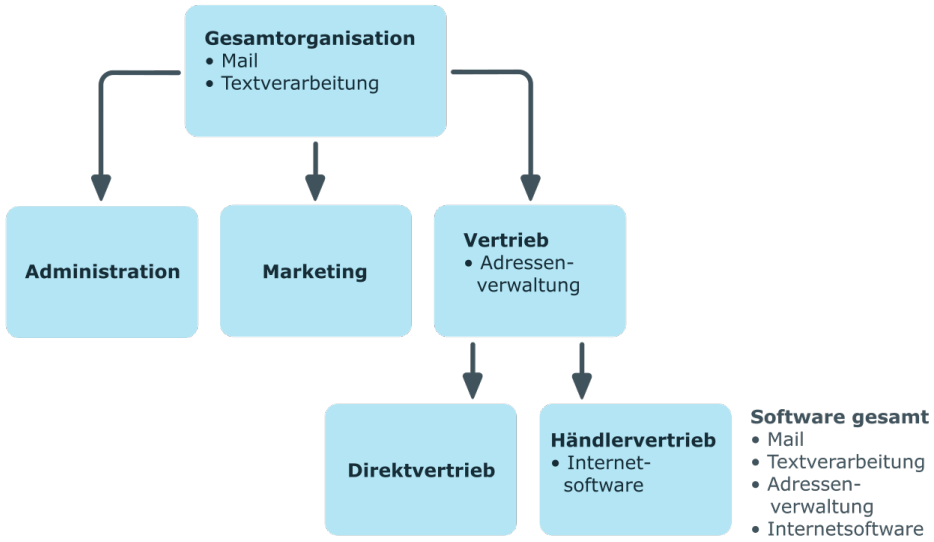
HINWEIS: Die Vererbungsrichtung wird nur bei der Vererbung von Unternehmensressourcen beachtet. Auf die Ermittlung der verantwortlichen Manager hat die Vererbungsrichtung keinen Einfluss. Der Manager einer übergeordneten Rolle ist immer für alle untergeordneten Rollen verantwortlich.

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

Beispiel für die Zuweisung von Unternehmensressourcen über Top-Down-Vererbung

Es wird ein Ausschnitt aus einer Unternehmensstruktur dargestellt. Zusätzlich sind Systemberechtigungen aufgeführt, die der jeweiligen Abteilung zugewiesen sind. Eine Person des Händlervertriebes erhält alle Systemberechtigungen, die ihrer Abteilung und allen Abteilungen auf dem Pfad zur Gesamtorganisation zugewiesen sind. In diesem Fall sind das die Azure Active Directory Gruppen 1 und 2 und die SharePoint Online Gruppen 1 und 2.

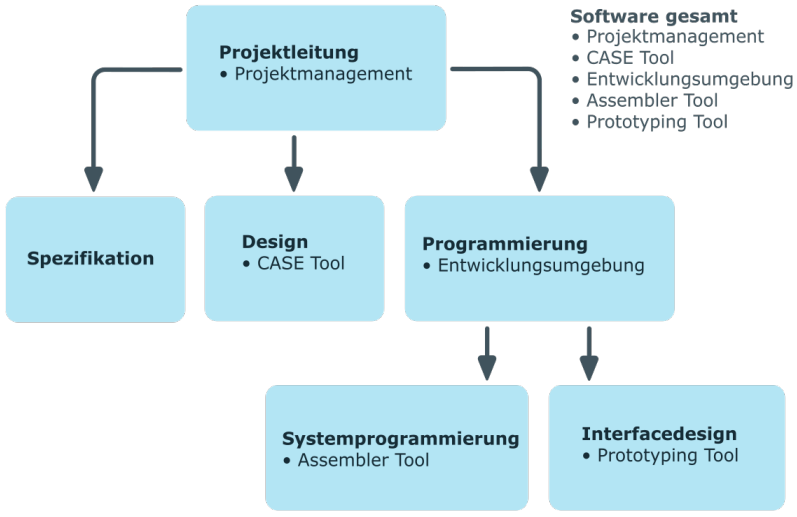
Abbildung 1: Zuweisung über Top-Down-Vererbung



Beispiel für die 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 für die Unterbrechung der Vererbung in einer Top-Down-Vererbung

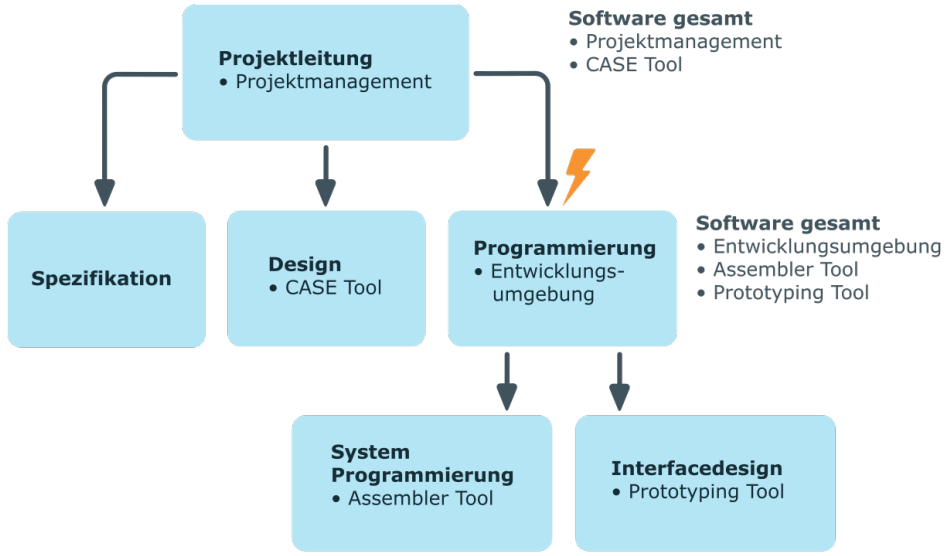
Wird im Beispiel einer Top-Down-Vererbung für die Abteilung "Vertrieb" die Option **Vererbung blockieren** gesetzt, hat das zur Folge, dass eine Person in der Abteilung "Vertrieb" nur die SharePoint Online Gruppe 1 und eine Person in der Abteilung "Händlervertrieb" die SharePoint Online Gruppe 1 und 2 erbt. Die Systemberechtigungen 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 für die 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



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
- Indirekte Zuweisung

- Zuweisung über dynamische Rollen
- Zuweisung über IT Shop Bestellungen

Direkte Zuweisung

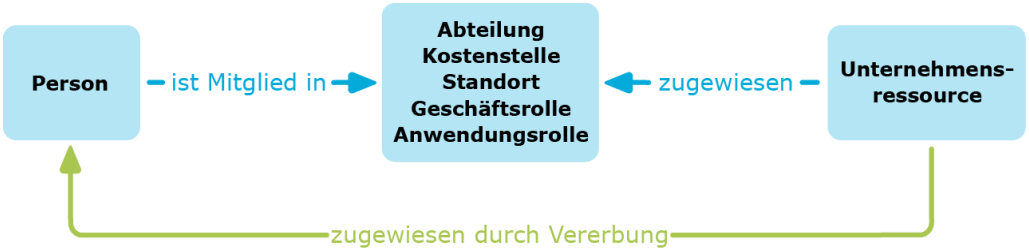
Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Person, einem Gerät oder einem Arbeitsplatz. Durch die direkte Zuweisung von Unternehmensressourcen kann ohne weiteren Aufwand auf Sonderanforderungen reagiert werden.

Abbildung 5: Schema einer direkten Zuweisung am Beispiel Person

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.

Abbildung 6: Schema einer indirekten Zuweisung am Beispiel Person



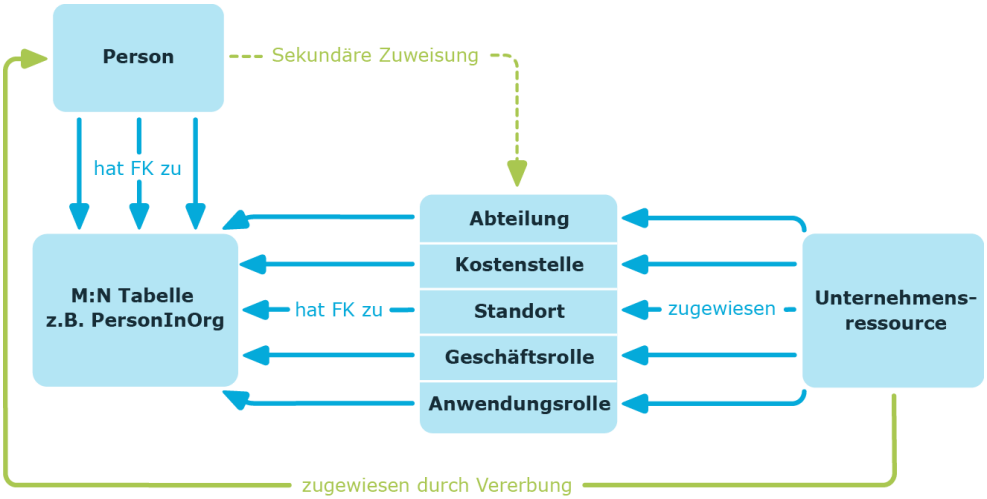
Verwandte Themen

- Sekundäre Zuweisung auf Seite 16
- Primäre Zuweisung auf Seite 16

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



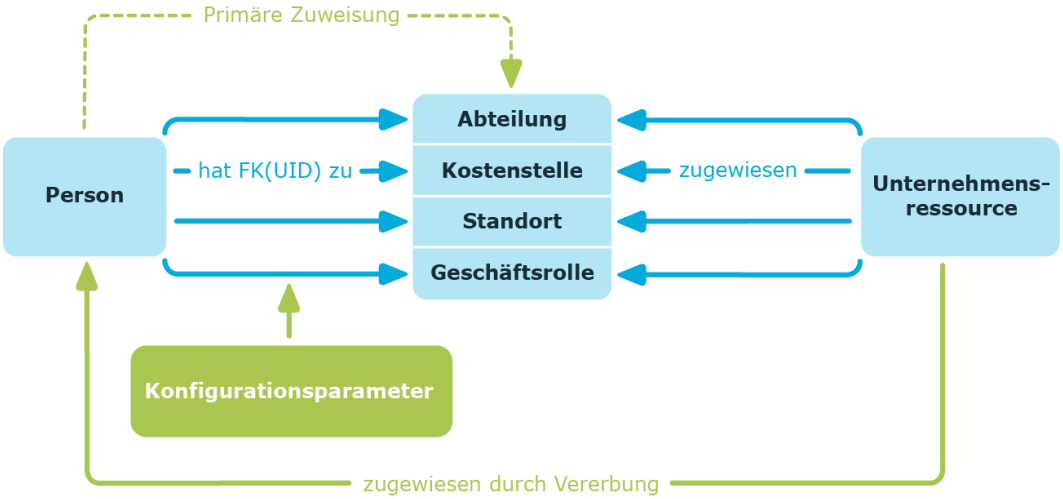
Verwandte Themen

- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26

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 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

- Arbeiten mit dynamischen Rollen auf Seite 66

Zuweisung über IT Shop Bestellungen

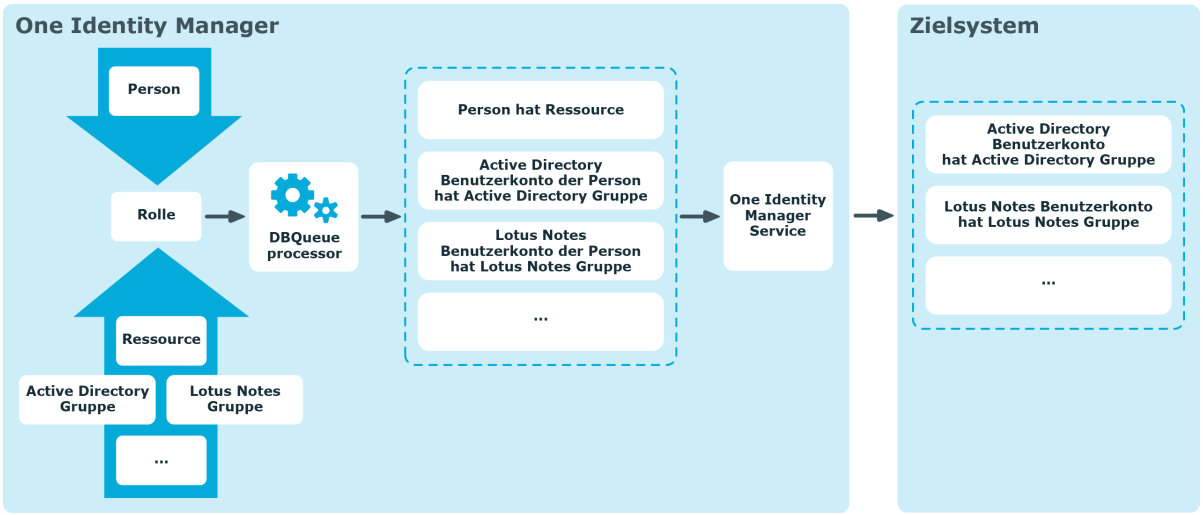
Die Zuweisung über IT Shop Bestellungen ist ein Spezialfall der indirekten Zuweisung. Damit Unternehmensressourcen über IT Shop Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Unternehmensressourcen, die als Produkte diesem Shop zugeordnet sind, können 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.

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 20
- Berechnung der Zuweisungen auf Seite 21

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. Das Datenmodell des One Identity Manager enthält 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:

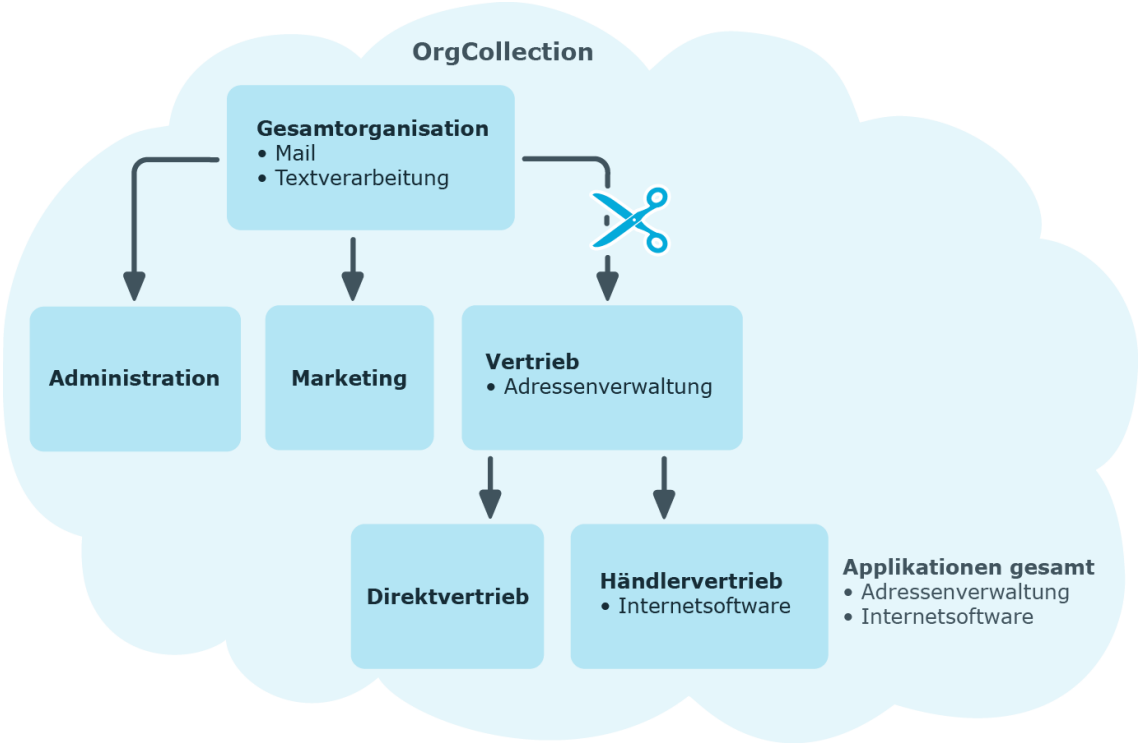
- UID_Org ist die Rolle, die erbt.
- UID_ParentOrg ist die Rolle, die vererbt.

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.

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)

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.

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.

Bit 3	Bit 2	Bit 1	Bit 0	Wert in XOrigin	Bedeutung
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.

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.
- 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 24
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26
- Einschränken der Vererbung über Rollen auf Seite 28
- Vererbungsausschluss: Festlegen widersprechender Rollen auf Seite 29

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)	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	Arbeitsplätze
Active Directory Gruppen	möglich (Zuweisung an alle Active Directory Benutzerkonten und Active Directory Kontakte einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
SharePoint Gruppen	möglich (Zuweisung an alle SharePoint Benutzerkonten einer Person)	-
SharePoint Rollen	möglich (Zuweisung an alle SharePoint Benutzerkonten einer Person)	-
LDAP Gruppen	möglich (Zuweisung an alle LDAP Benutzerkonten einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
Notes Gruppen	möglich (Zuweisung an alle Notes Benutzerkonten einer Person)	-
SAP Gruppen	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen)	-
SAP Profile	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen)	-
SAP Rollen	möglich (Zuweisung an alle SAP Benutzerkonten einer Person, die im selben SAP Mandanten liegen)	-
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)	-
BI Analyseberechtigungen	möglich (Zuweisung an alle BI Benutzerkonten einer Person, die im selben System liegen)	-
Azure Active Directory Gruppen	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	Arbeitsplätze
Azure Active Directory Administratorrollen	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
Azure Active Directory Abonnements	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
Unwirksame Azure Active Directory Dienstpläne	möglich (Zuweisung an alle Azure Active Directory Benutzerkonten einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
Unix Gruppen	möglich (Zuweisung an alle Unix Benutzerkonten einer Person)	-
PAM Benutzergruppen	möglich (Zuweisung an alle PAM Benutzerkonten einer Person, für welche die Vererbung von Gruppen zugelassen ist)	-
Systemrollen	möglich	möglich
Abonnierbare Berichte	möglich	-
Software	möglich	möglich

Verwandte Themen

- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54

Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen 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.

Um die sekundäre Zuweisung zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie unter **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.

Einschränken der Vererbung über Rollen

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 zu unterbrechen

1. Öffnen Sie das Stammdatenformular für eine Rolle.
2. Aktivieren Sie die Option **Vererbung blockieren**.
3. Speichern Sie die Änderungen.

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 eine Rolle zu verhindern

1. Öffnen Sie das Stammdatenformular für die Rolle.
2. 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**.
3. Speichern Sie die Änderungen.

Ebenso kann für einzelne Personen, Geräte oder Arbeitsplätze 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. Öffnen Sie das Stammdatenformular für die Person.
2. 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.
3. Speichern Sie die Änderungen.

Um die Vererbung für ein Gerät zu verhindern

1. Öffnen Sie das Stammdatenformular für das Gerät.
2. 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.
3. Speichern Sie die Änderungen.

Um die Vererbung für einen Arbeitsplatz zu verhindern

1. Öffnen Sie das Stammdatenformular für den Arbeitsplatz.
2. 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.
3. Speichern Sie die Änderungen.

Verwandte Themen

- Unterbrechen der Vererbung auf Seite 13

Vererbungsausschluss: Festlegen widersprechender Rollen

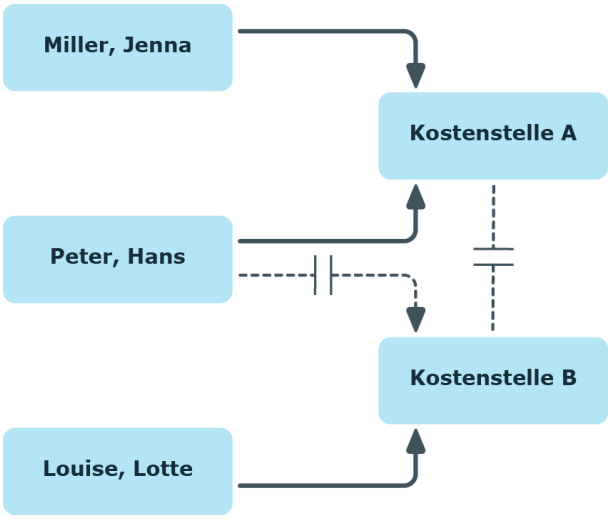
Um zu verhindern, dass Personen, Geräte oder Arbeitsplätze gleichzeitig an verschiedene Rollen zugewiesen werden und über diese Rollen sich ausschließende Unternehmensressourcen erhalten könnten, können Sie widersprechende Rollen definieren. Dabei legen Sie fest, welche Anwendungsrollen, Abteilungen, 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.

Verwandte Themen

- Vererbungsausschluss für Rollen festlegen auf Seite 63

Abteilungen, Kostenstellen und Standorte verwalten

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 Software. 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

- Abteilungen bearbeiten auf Seite 40
- Kostenstellen bearbeiten auf Seite 44
- Standorte bearbeiten auf Seite 48
- Einrichten der IT Betriebsdaten auf Seite 56
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Vorbereiten der hierarchische Rollen für die Zuweisung von Unternehmensressourcen auf Seite 23

One Identity Manager Benutzer für Organisationen

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

Tabelle 5: 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. • Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
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. 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

Benutzer	Aufgaben
	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.

Basisdaten zum Aufbau von Abteilungen, Kostenstellen und Standorten

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.

- 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. Im One Identity Manager ist eine Standardanwendungsrolle für Attestierer vorhanden. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, Berechtigungen, Bestellungen oder andere im One Identity Manager gespeicherte Daten zu attestieren. 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*.

- 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. Im One Identity Manager sind Standardanwendungsrollen für Genehmiger und Genehmiger (IT) vorhanden. Diesen Anwendungsrollen weisen Sie die Personen zu, die berechtigt sind, Bestellungen im IT Shop zu genehmigen. 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 auf Seite 35
- Rollentypen auf Seite 35
- Unternehmensbereiche auf Seite 36
- Attestierer auf Seite 37
- Genehmiger und Genehmiger (IT) auf Seite 38
- Konfigurationsparameter für die Verwaltung von Abteilungen, Kostenstellen und Standorten auf Seite 192

Rollenklassen

Rollenklassen bilden die Basis für die Abbildung von hierarchischen Rollen im One Identity Manager. Rollenklassen dienen zur Zusammenfassung gleichartiger Rollen. Folgende Rollenklassen sind standardmäßig für die Abbildung von Organisationen im One Identity Manager vorhanden:

- Abteilung
- Kostenstelle
- Standort

An der Rollenklasse ist die Vererbungsrichtung festgelegt. Für Abteilungen, Kostenstellen, Standorte und Anwendungsrollen ist eine Top-Down Vererbung definiert. Zusätzlich wird für die Rollenklasse festgelegt, welche Zuweisungen an die einzelnen Rollen erlaubt sind. 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 10
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26

Rollentypen

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

Um Rollentypen zu bearbeiten

1. Wählen Sie die Kategorie **Organisationen | Basisdaten zur Konfiguration | Rollentypen**.
2. Wählen Sie in der Ergebnisliste einen Rollentyp aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Für einen Rollentyp erfassen Sie die folgenden Stammdaten.

Tabelle 6: Eigenschaften für Rollentypen

Eigenschaft	Beschreibung
Rollentyp	Bezeichnung des Rollentyps.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Unternehmensbereiche

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.

Beispiel für den 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 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 7: 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.
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.

Verwandte Themen

- One Identity Manager Administrationshandbuch für Complianceregeln

Attestierer

Installierte Module: Modul Attestierung

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. Im One Identity Manager ist eine Standardanwendungsrolle für Attestierer vorhanden. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, Berechtigungen, Bestellungen oder andere im One Identity Manager gespeicherte Daten zu attestieren. 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 8: Standardanwendungsrolle für Attestierer

Benutzer	Aufgaben
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.

Um Attestierer festzulegen

1. Wählen Sie 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.

Verwandte Themen

- One Identity Manager Administrationshandbuch für Attestierungen

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. Im One Identity Manager sind Standardanwendungsrollen für Genehmiger und Genehmiger (IT) vorhanden. Diesen Anwendungsrollen weisen Sie die Personen zu, die berechtigt sind, Bestellungen im IT Shop zu genehmigen. 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 9: 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 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 die Kategorie **Organisationen | Basisdaten zur Konfiguration | Genehmiger**.

   - ODER -

   Wählen Sie 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.

   - ODER -

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

Verwandte Themen

- One Identity Manager Administrationshandbuch für IT Shop

Abteilungen bearbeiten

Um Abteilungen zu bearbeiten

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.
2. Wählen Sie in der Ergebnisliste eine Abteilung aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Abteilung auf Seite 40
- Kontaktinformationen einer Abteilung auf Seite 43
- Unternehmensbereich und Risikobewertung auf Seite 43
- Einrichten der IT Betriebsdaten auf Seite 56

Allgemeine Stammdaten einer Abteilung

Für eine Abteilung erfassen Sie die folgenden allgemeine Stammdaten.

Tabelle 10: Allgemeine Stammdaten einer Abteilung

Eigenschaft	Beschreibung
Abteilung	Bezeichnung der Abteilung.
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.
Rollentyp	Rollentyp zur weiteren Klassifizierung.

Eigenschaft	Beschreibung
Standort	Standort, dem die Abteilung primär zugeordnet ist.
Standard-Druck-server	Standarddrucker der Abteilung. Um der Abteilung einen Druckserver zuzuordnen, wählen Sie einen Server aus der Auswahlliste aus. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.
Manager	Verantwortlicher Manager der Abteilung.
2. Verantwortlicher	Stellvertretender Manager der Abteilung.
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

Eigenschaft	Beschreibung
	einen Manager nicht genehmigt.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Vollständiger Name	Vollständige Bezeichnung der Abteilung inklusive der übergeordneten Abteilungen.
Deaktiviert	Angabe, ob die Abteilung aktiv genutzt wird. Aktivieren Sie diese Option, wenn die Abteilung nicht genutzt wird. Die Option hat keinen Einfluss auf die Berechnung der Vererbung.
Vererbung blockieren	Angabe, 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	Angabe, ob die Vererbung an Personen für die Abteilung vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Angabe, ob die Vererbung an Geräte für die Abteilung vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Angabe, ob die Vererbung an Arbeitsplätze für die Abteilung vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Angabe, 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 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 auf Seite 35
- Attestierer auf Seite 37
- Genehmiger und Genehmiger (IT) auf Seite 38
- Einschränken der Vererbung über Rollen auf Seite 28
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen auf Seite 61

Kontaktinformationen einer Abteilung

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

Tabelle 12: 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.
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen an die Abteilung sind. Stellen Sie über den Schieberegler einen Wert zwischen 0 und 1 ein.

Eigenschaft	Beschreibung
	0 ... keine Transparenz 1 ... volle Transparenz
Max. Anzahl Regelverletzungen	Legen Sie fest, wie viele Regelverletzungen in dieser Abteilung zulässig sind. Der Wert kann bei der Prüfung von Complianceregeln ausgewertet werden. 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 einer Person auf Seite 133
- Ermitteln der Arbeitszeit einer Person auf Seite 134
- Unternehmensbereiche auf Seite 36
- One Identity Manager Administrationshandbuch für Risikobewertungen
- One Identity Manager Administrationshandbuch für Complianceregeln

Kostenstellen bearbeiten

Um Kostenstellen zu bearbeiten

1. Wählen Sie die Kategorie **Organisationen | Kostenstellen**.
2. Wählen Sie in der Ergebnisliste eine Kostenstelle aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kostenstelle auf Seite 45
- Unternehmensbereich und Risikobewertung auf Seite 47
- Einrichten der IT Betriebsdaten auf Seite 56

Allgemeine Stammdaten einer Kostenstelle

Für eine Kostenstelle erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 13: Allgemeine Stammdaten einer Kostenstelle

Eigenschaft	Beschreibung
Kostenstelle	Bezeichnung der Kostenstelle.
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.
Rollentyp	Rollentyp zur weiteren Klassifizierung.
Manager	Verantwortlicher Manager der Kostenstelle.
2. Verantwortlicher	Stellvertretender Manager der Kostenstelle.
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.
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.

Eigenschaft	Beschreibung
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.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Deaktiviert	Angabe, 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	Angabe, 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	Angabe, ob die Vererbung an Personen für die Kostenstelle vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Angabe, ob die Vererbung an Geräte für die Kostenstelle vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Angabe, ob die Vererbung an Arbeitsplätze für die Kostenstelle vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Angabe, 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 auf Seite 35
- Attestierer auf Seite 37

- Genehmiger und Genehmiger (IT) auf Seite 38
- Einschränken der Vererbung über Rollen auf Seite 28
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen auf Seite 61

Unternehmensbereich und Risikobewertung

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

Tabelle 14: Stammdaten zum Unternehmensbereich einer Kostenstelle

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 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.
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	Legen Sie fest, wie viele Regelverletzungen in dieser Kostenstelle zulässig sind. Der Wert kann bei der Prüfung von Complianceregeln ausgewertet werden. 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 einer Person auf Seite 133
- Ermitteln der Arbeitszeit einer Person auf Seite 134
- Unternehmensbereiche auf Seite 36
- One Identity Manager Administrationshandbuch für Risikobewertungen
- One Identity Manager Administrationshandbuch für Complianceregeln

Standorte bearbeiten

Um Standorte zu bearbeiten

1. Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste einen Standort aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Standorts auf Seite 48
- Adressinformationen eines Standorts auf Seite 51
- Netzwerkkonfiguration eines Standorts auf Seite 51
- Anfahrtsbeschreibung eines Standorts auf Seite 52
- Unternehmensbereich und Risikobewertung auf Seite 52
- Einrichten der IT Betriebsdaten auf Seite 56

Allgemeine Stammdaten eines Standorts

Für einen Standort erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 15: Allgemein Stammdaten eines Standortes

Eigenschaft	Beschreibung
Standort	Bezeichnung des Standorts.

Eigenschaft	Beschreibung
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.
Rollentyp	Rollentyp zur weiteren Klassifizierung.
Manager	Verantwortlicher Manager des Standorts.
2. Verantwortlicher	Stellvertretender Manager des Standorts.
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 Zertifizierungsstatus können ausgewählt werden.

Eigenschaft	Beschreibung
	• 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.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Deaktiviert	Angabe, 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	Angabe, 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	Angabe, ob die Vererbung an Personen für den Standort vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Angabe, ob die Vererbung an Geräte für den Standort vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Angabe, ob die Vererbung an Arbeitsplätze für den Standort vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Angabe, 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 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 auf Seite 35
- Attestierer auf Seite 37
- Genehmiger und Genehmiger (IT) auf Seite 38
- Einschränken der Vererbung über Rollen auf Seite 28
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen auf Seite 61

Adressinformationen eines Standorts

Erfassen Sie die folgenden Stammdaten zur Erreichbarkeit des Standorts.

Tabelle 16: 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 einer Person auf Seite 133
- Ermitteln der Arbeitszeit einer Person auf Seite 134

Netzwerkkonfiguration eines Standorts

Erfassen Sie Informationen über die Konfiguration des Netzwerkes am Standort.

Tabelle 17: Netzwerkinformationen eines Standorts

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

Anfahrtsbeschreibung eines Standorts

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 18: Anfahrtsbeschreibung eines Standorts

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

Unternehmensbereich und Risikobewertung

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

Tabelle 19: Stammdaten zum Unternehmensbereich eines Standorts

Eigenschaft	Beschreibung
Unternehmensbereich	Unternehmensbereich des Standorts. Die Angabe wird zur 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.
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	Legen Sie fest, wie viele Regelverletzungen in diesem Standort zulässig sind. Der Wert kann bei der Prüfung von Complianceregeln ausgewertet werden. 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 auf Seite 36
- One Identity Manager Administrationshandbuch für Risikobewertungen
- One Identity Manager Administrationshandbuch für Complianceregeln

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 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.

    - ODER -

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

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

Verwandte Themen

- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen auf Seite 61
- Personen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 119
- Geräte an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 152
- Arbeitsplatz an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 160

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 20: Mögliche Zuweisungen von Unternehmensressourcen an Rollen

Unternehmensressource	Verfügbar im Modul
Ressourcen	immer
Kontendefinitionen	Zielsystem Basismodul

Unternehmensressource	Verfügbar im Modul
Gruppen kundendefinierter Zielsysteme	Zielsystem Basismodul
Active Directory Gruppen	Active Directory Modul
SharePoint Gruppen	SharePoint Modul
SharePoint Rollen	SharePoint Modul
LDAP Gruppen	LDAP Modul
Notes Gruppen	IBM Notes 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-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 Dienstpläne	Azure Active Directory Modul
Unix Gruppen	Modul Unix-basierte Zielsysteme
Cloud Gruppen	Modul Cloud Systems Management
PAM Benutzergruppen	Privileged Account Governance Modul
G Suite Gruppen	G Suite Modul
G Suite Produkte und SKUs	G Suite Modul

Um Unternehmensressourcen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie 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.

   - ODER -

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

Detaillierte Informationen zum Thema

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 24
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Arbeiten mit dynamischen Rollen auf Seite 66

Einrichten der IT Betriebsdaten

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

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

Beispiel

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

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten der Domäne A und eine Kontendefinition B für die administrativen Benutzerkonten der Domäne A.

In der Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft "Abteilung" zur Ermittlung der gültigen IT Betriebsdaten fest.

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager 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.

Tabelle 21: IT Betriebsdaten

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

5. Speichern Sie die Änderungen.

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
IBM Notes	Server
	Zertifikat
	Vorlage der Postdatei
	Identität
SharePoint	Authentifizierungsmodus
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
SharePoint Online	Gruppen erbbar
	Privilegiertes Benutzerkonto
	Authentifizierungsmodus

Zielsystemtyp	IT Betriebsdaten
Kundendefinierte Zielsysteme	Container (je Zielsystem)
	Gruppen erbbar
	Identität
	Privilegiertes Benutzerkonto
Azure Active Directory	Gruppen 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
Exchange Online	Gruppen erbbar
Privileged Account Management	Authentifizierungsanbieter
	Identität
	Gruppen erbbar
	Privilegiertes Benutzerkonto
G Suite	Organisation
	Identität
	Gruppen erbbar
	Privilegiertes Benutzerkonto
	Kennwort bei der nächsten Anmeldung ändern

Verwandte Themen

- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul

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.

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

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

5. Klicken Sie **Übernehmen**.

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zusätzliche Aufgaben zur Verwaltung von Abteilungen, Kostenstellen und Standorten

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

Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen

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 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 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

- Arbeiten mit dynamischen Rollen auf Seite 66
- Dynamische Rollen bearbeiten auf Seite 67
- Allgemeine Stammdaten einer Abteilung auf Seite 40
- Allgemeine Stammdaten einer Kostenstelle auf Seite 45
- Allgemeine Stammdaten eines Standorts auf Seite 48

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 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.

   - ODER -

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

Um eine Abteilung oder einen Standort an Kostenstellen zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

Um eine Abteilung oder eine Kostenstelle an Standorte zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

Vererbungsausschluss für Rollen 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 Anwendungsrollen, 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.

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 29

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 23: 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 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**.

Verwandte Themen

- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 127

Arbeiten mit dynamischen Rollen

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.

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.

Beispiel für die 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.

Detaillierte Informationen zum Thema

- Dynamische Rollen bearbeiten auf Seite 67
- Berechnung der Rollenmitgliedschaften auf Seite 70

Verwandte Themen

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26
- Konfigurationsparameter für die Verwaltung von Abteilungen, Kostenstellen und Standorten auf Seite 192

Dynamische Rollen 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 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 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

- Dynamische Rollen für Abteilungen, Kostenstellen und Standorte erstellen auf Seite 61
- Ausführliche Informationen zu dynamischen Rollen für Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Stammdaten einer dynamischen Rolle

Für eine dynamische Rolle erfassen Sie die folgenden Daten.

Tabelle 24: 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 unikal 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. In der Standardinstallation des One Identity Managers ist bereits der Zeitplan **Berechnung dynamischer Rollen** definiert. Durch diesen Zeitplan werden die Rollenmitgliedschaften für alle dynamischen Rollen geprüft und nötigenfalls Aufträge zur Neuberechnung für den DBQueue Prozessor eingestellt. Um Zeitpläne an Ihre Erfordernisse anzupassen oder neue Zeitpläne einzurichten, verwenden Sie den Designer. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bedingung	Definiert, welche Objekte der Objektklasse Mitglieder der ausgewählten Rolle werden. Weitere Informationen finden Sie unter Bedingungen für dynamische Rollen auf Seite 69.

Ausführliche Informationen zur Bedienung des Where-Klausel Assistenten und Filterdesigners finden Sie im *One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge*.

Verwandte Themen

- Dynamische Rollen bearbeiten auf Seite 67
- Bedingung einer dynamischen Rolle testen auf Seite 69
- Sofortige Neuberechnung der Rollenmitgliedschaften veranlassen auf Seite 72

Bedingungen für dynamische Rollen

Die Bedingung einer dynamischen Rolle wird als gültige `Where`–Klausel für Datenbankabfragen definiert und muss sich auf die gewählte Objektklasse beziehen.

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

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.

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.

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

- Bedingung einer dynamischen Rolle testen auf Seite 69

Bedingung einer dynamischen Rolle testen

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

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

Um die SQL-Bedingung zu testen

1. Wählen Sie 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.

Berechnung der Rollenmitgliedschaften

Tabelle 25: Konfigurationsparameter für die Berechnung dynamischer Rollen

Konfigurationsparameter	Bedeutung
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. 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.

Um 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
- mindestens ein Objekt gibt, das der Bedingung nicht genügt, aber der Rolle zugeordnet ist

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

Je nach Einstellung der Konfigurationsparameter werden Aufträge zur Neuberechnung der Mitgliedschaften eingestellt durch:

- die zyklische Überprüfung über einen Zeitplan

  In der Standardinstallation des One Identity Manager ist bereits der Zeitplan **Berechnung dynamischer Rollen** definiert. Durch diesen 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. Um Zeitpläne an Ihre Erfordernisse anzupassen oder neue Zeitpläne einzurichten, verwenden Sie den Designer. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
- sofort bei Änderung eines Objektes

  Die Mitgliedschaften werden bei jeder Eigenschaftsänderung der Objekte sofort durch den DBQueue Prozessor überprüft und nötigenfalls geändert. Um diese Funktion zu nutzen, aktivieren Sie im Designer die Konfigurationsparameter **QER | Structures | DynamicGroupCheck | CalculateImmediatelyPerson**, **QER | Structures | DynamicGroupCheck | CalculateImmediatelyHardware** und **QER | Structures | DynamicGroupCheck | CalculateImmediatelyWorkdesk**.

Verwandte Themen

- Sofortige Neuberechnung der Rollenmitgliedschaften veranlassen auf Seite 72

Zusätzliche Aufgaben für dynamische Rollen

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

Überblick über eine dynamische Rolle

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 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 **Überblick über die dynamische Rolle**.

Sofortige Neuberechnung der Rollenmitgliedschaften veranlassen

Standardmäßig wird die Berechnung der Rollenmitgliedschaften über Zeitpläne gesteuert. Sie können die Berechnung für eine einzelne dynamische Rolle auch sofort und unabhängig von der zyklischen Berechnung veranlassen.

Um Rollenmitgliedschaften sofort zu berechnen

1. Wählen Sie 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 **Neuberechnung sofort veranlassen** und schließen Sie die Meldung mit **OK**.

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

Detaillierte Informationen zum Thema

- Berechnung der Rollenmitgliedschaften auf Seite 70

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

- Erfassen der Personenstammdaten auf Seite 82
- Deaktivieren und Löschen von Personen auf Seite 97
- Unternehmensressourcen an Personen zuweisen auf Seite 115
- Herkunft von Rollen und Berechtigungen einer Person anzeigen auf Seite 125
- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 127
- Abbildung mehrerer Identitäten einer Person auf Seite 95
- Eingeschränkter Zugang zum One Identity Manager auf Seite 113
- Berichte über Personen auf Seite 135

One Identity Manager Benutzer für die Personenverwaltung

In die Verwaltung von Personen sind folgende Benutzer eingebunden.

Tabelle 26: 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 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.
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 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. Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.

Benutzer	Aufgaben
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

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

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 auf Seite 76
- Unternehmensspezifische Mailvorlagen für Benachrichtigungen erstellen auf Seite 77
- Kennwortrichtlinien für Personen auf Seite 101
- Konfigurationsparameter für die Verwaltung von Personen auf Seite 195

Partnerfirmen

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

Um die Stammdaten für eine Partnerfirma zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Personen | Basisdaten zur Konfiguration | Partnerfirmen**.
2. Wählen Sie in der Ergebnisliste eine Firma aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 27: 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.

Eigenschaft	Beschreibung
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 28: 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 **Browsen** wird die angegebene Webseite im Standardwebbrowser angezeigt.

Unternehmensspezifische Mailvorlagen für Benachrichtigungen erstellen

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.

Zur einfachen Erstellung von Benachrichtigungen ist im One Identity Manager ein Mailvorlageneditor integriert. Mit dem Mailvorlageneditor können Sie Mailtexte im WYSIWYG-Modus erstellen und bearbeiten.

Um Mailvorlagen 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**.

Detaillierte Informationen zum Thema

- Erstellen und Bearbeiten einer Maildefinition auf Seite 80
- Anpassen der E-Mail Signatur auf Seite 81

Allgemeine Eigenschaften einer Mailvorlage

Für eine Mailvorlage werden die folgenden allgemeinen Eigenschaften abgebildet.

Tabelle 29: Eigenschaften einer Mailvorlage

Eigenschaft	Bedeutung
Mailvorlage	Bezeichnung der Mailvorlage. Mit dieser Bezeichnung werden die Mailvorlagen in den Administrationswerkzeugen und im Web Portal angezeigt. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Basisobjekt	Basisobjekt der Mailvorlage. Die Angabe eines Basisobjekts ist nur erforderlich, wenn in der Maildefinition Eigenschaften des Basisobjekts referenziert werden.
Bericht (Parametersatz)	Bericht, der über die Mailvorlage zur Verfügung gestellt wird.
Beschreibung	Beschreibung der Mailvorlage. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Zielformat	Format, in dem die E-Mail Benachrichtigung generiert wird. Zulässige Werte sind: • **HTML**: Die E-Mail Benachrichtigung wird als HTML formatiert. Im HTML-Format können Textformatierungen wie beispielsweise unterschiedliche Schriftarten, farbige Schriften oder andere Textformatierungen enthalten sein. • **TXT**: Die E-Mail Benachrichtigung wird als Text formatiert. Das Text-Format unterstützt keine fetten, kursiven oder farbige Schriften oder andere Textformatierungen. Bilder, die direkt in der Benachrichtigung angezeigt werden, werden ebenfalls nicht unterstützt.
Designtyp	Design, in welchem die E-Mail Benachrichtigung generiert wird. Zulässige Werte sind: • **Mailvorlage**: Die generierte E-Mail Benachrichtigung enthält den Mailbody entsprechend der Maildefinition. • **Bericht**: Die generierte E-Mail Benachrichtigung enthält den unter **Bericht (Parametersatz)** angegebenen Bericht als Mailbody. • **Mailvorlage, Bericht im Anhang**: Die generierte E-Mail Benach-

Eigenschaft	Bedeutung
	richtigung enthält den Mailbody entsprechend der Maildefinition. Der unter **Bericht (Parametersatz)** angegebene Bericht wird als PDF-Datei an die Benachrichtigung angehängt.
Wichtigkeit	Wichtigkeit für die E-Mail Benachrichtigung. Zulässig sind die Werte **Niedrig**, **Normal** und **Hoch**.
Vertraulichkeit	Vertraulichkeit für die E-Mail Benachrichtigung. Zulässig sind die Werte **Normal**, **Persönlich**, **Privat** und **Vertraulich**.
Abbestellen erlaubt	Angabe, ob ein Empfänger die E-Mail Benachrichtigung abbestellen kann. Ist die Option aktiviert, kann die E-Mail Benachrichtigung über das Web Portal abbestellt werden.
Deaktiviert	Angabe, ob diese Mailvorlage deaktiviert ist.
Maildefinition	Eindeutige Bezeichnung der Maildefinition.
Sprachkultur	Sprachkultur, für welche die Mailvorlage gelten soll. Bei Generierung einer E-Mail-Benachrichtigung werden die Spracheinstellungen des Empfängers berücksichtigt.
Betreff	Betreff der E-Mail Benachrichtigung.
Mailbody	Inhalt der E-Mail Benachrichtigung.

Erstellen und Bearbeiten einer Maildefinition

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. Öffnen Sie die Mailvorlage im Mailvorlageneditor.
2. Klicken Sie die Schaltfläche neben der Auswahlliste **Maildefinition**.
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. Öffnen Sie die Mailvorlage im Mailvorlageneditor.
2. Wählen Sie in der Auswahlliste **Maildefinition** die Sprache.
3. Bearbeiten Sie die Betreffzeile und den Mailbody.
4. Speichern Sie die Änderungen.

Eigenschaften des Basisobjekts verwenden

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*.

Anpassen der E-Mail Signatur

Die E-Mail Signatur für die Mailvorlagen konfigurieren Sie über die folgenden Konfigurationsparameter. Die Konfigurationsparameter bearbeiten Sie im Designer.

Tabelle 30: Konfigurationsparameter für die E-Mail Signatur

Konfigurationsparameter	Beschreibung
Common | MailNotification | Signature	Angaben zur Signatur in automatisch aus Mailvorlagen generierten E-Mails.
Common | MailNotification | Signature | Caption	Unterschrift unter die Grußformel.
Common | MailNotification | Signature | Company	Name des Unternehmens.
Common | MailNotification | Signature | Link	Link zur Firmenwebseite.
Common | MailNotification | Signature | LinkDisplay	Anzeigetext für den Link zur Firmenwebseite.

Das Skript `VI_GetRichMailSignature` stellt die Bestandteile einer E-Mail Signatur entsprechend der Konfigurationsparameter zur Verwendung in Mailvorlagen zusammen.

Erfassen der Personenstammdaten

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 One Identity 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 Personenstammdaten 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 Mastersystem ist. Welche Eigenschaften gesperrt sind, ist von der Datenquelle abhängig, aus der die Personenstammdaten importiert wurden.

Detaillierte Informationen zum Thema

- Allgemeine Personenstammdaten auf Seite 83
- Organisatorische Personenstammdaten auf Seite 85

- Adressenangaben auf Seite 87
- Sonstige Personenstammdaten auf Seite 89

Allgemeine Personenstammdaten

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

Tabelle 31: 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 wird ebenfalls für die Anzeige des Web Portals genutzt.
Unterorganisation	Vermerk, welcher Unterorganisation die Person angehört.
Dauerhaft deaktiviert	Angabe, ob die Person aktuell ein Mitarbeiter Ihres

Eigenschaft	Beschreibung
	Unternehmens ist. Ist die Option aktiviert, ist die Person als Mitarbeiter ausgeschieden. Ihr wurden alle Berechtigungen als One Identity Manager Benutzer entzogen.
Zertifizierungsstatus	Angabe, 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	Angabe, ob die Person für Ihr Unternehmen als sicherheitsgefährdend eingestuft ist. Bei entsprechender Konfiguration wird die Vererbung von Ressourcen und Berechtigungen an derart gekennzeichnete Personen unterbunden und die Benutzerkonten werden gesperrt.
Keine Vererbung	Angabe, ob die Person Unternehmensressourcen über Rollen 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	Angabe, 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**.

Eigenschaft	Beschreibung
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 einer Person ändern auf Seite 114
- Dauerhafte Deaktivierung einer Person auf Seite 98
- Einschränken der Vererbung über Rollen auf Seite 28
- Partnerfirmen auf Seite 76
- Einrichten von Arbeitsplätzen auf Seite 155

Organisatorische Personenstammdaten

Für Personen erfassen Sie die folgenden organisatorischen Stammdaten.

Tabelle 32: Organisatorische Stammdaten

Eigenschaft	Beschreibung
Personalnummer	Personalnummer der Person.

Eigenschaft	Beschreibung
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.
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.

Eigenschaft	Beschreibung
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 noch einige Zeit 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 • 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 23
- Dauerhafte Deaktivierung einer Person auf Seite 98
- Zeitweilige Deaktivierung einer Person auf Seite 98

Adressenangaben

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

Tabelle 33: 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	Angabe, ob die Person im Telefonbuch angezeigt wird.
Straße	Straße.
Gebäude	Gebäude.
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 23
- Ermitteln der Sprache einer Person auf Seite 133
- Ermitteln der Arbeitszeit einer Person auf Seite 134

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 34: 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 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

Eigenschaft	Beschreibung
	Manager verwendet werden. Abhängig von der Konfiguration wird dazu das zentrale Kennwort einer Person an ihre Benutzerkonten und auf ihr Systembenutzerkennwort publiziert.
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.
Dummy-Person	Gibt an, ob die Person eine wirkliche Person darstellt oder eine Dummy-Person, die beispielsweise für die Verbindung mit administrativen Benutzerkonten genutzt wird.
Wirkliche Person	Eindeutige Kennung der wirklichen Person.
X500-Dummy	Gibt an, ob die Person als X500-Dummy-Person im One Identity Manager geführt wird. Hat eine Person mehrere X500-Einträge, die sich in einzelnen Eigenschaften unterscheiden, so können Sie hier ebenfalls Dummy-Personen nutzen. Für den Anwendungsfall kennzeichnen Sie die Person mit der Option **X500-Dummy** und stellen eine Verknüpfung zur wirklichen X500-Person her.
X500-Person	Ordnen Sie der X500-Dummy-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.

Eigenschaft	Beschreibung
	Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
Starling 2FA Benutzerkennung	Benutzerkennung für die Multifaktor-Authentifizierung. Ausführliche Informationen zur Multifaktor-Authentifizierung finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
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.
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	Angabe, ob der Person die Anmeldung am Terminalserver mit ihrem Benutzerkonto erlaubt ist.
Remote-Zugriff erlaubt	Angabe, ob sich die Person mit ihrem Benutzerkonto remote in das Netzwerk einwählen darf.
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.
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 92
- Zentrales Kennwort einer Person auf Seite 93
- Standard-E-Mail-Adresse einer Person auf Seite 94

- Abbildung mehrerer Identitäten einer Person auf Seite 95
- Identitätstypen von Personen auf Seite 96

Zentrales Benutzerkonto einer Person

Tabelle 35: Konfigurationsparameter für die Bildung der zentralen Benutzerkonten

Konfigurationsparameter	Bedeutung
QER | Person | CentralAccountGlobalUnique	Der Konfigurationsparameter 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 Zielsystemen. 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 36: Beispiel für die Bildung des zentralen Benutzerkontos

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

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 ebenfalls für neue Benutzerkonten der Person zu nutzen, aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | UseCentralPassword | PermanentStore**.

  Ist der Konfigurationsparameter aktiviert, wird das zentrale Kennwort in der One Identity Manager-Datenbank gespeichert und wird für neue Benutzerkonten genutzt. Ist der Konfigurationsparameter deaktiviert, wird das zentrale Kennwort nach dem Publizieren an die bestehenden Benutzerkonten aus der One Identity Manager-Datenbank gelöscht werden. Das zentrale Kennwort steht für weitere Benutzerkonten nicht zur Verfügung.
- 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 nicht auf privilegierte Benutzerkonten der Person publiziert.
- Kann ein Kennwortes aufgrund eines Fehlers nicht geändert werden, erhält die Person eine entsprechenden 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 kann über das Kennwortrücksetzungsportal gesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal* und im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Verwandte Themen

- Sonstige Personenstammdaten auf Seite 89
- Kennwortrichtlinien für Personen auf Seite 101
- Kennwortfragen festlegen auf Seite 131
- Nachbarschaftshilfe auf Seite 132
- Gesperrte Personen und Systembenutzer anzeigen auf Seite 113

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 92

Abbildung mehrerer Identitäten einer Person

Tabelle 37: Konfigurationsparameter für die Abbildung mehrerer Identitäten

Konfigurationsparameter	Wirkung bei Aktivierung
Person | MasterIdentity | UseMasterForAuthentication	Der Konfigurationsparameter legt fest, ob zur Anmeldung an One Identity Manager-Werkzeugen über Personen-basierte 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. 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 Abteilungs- oder Kostenstellenzugehörigkeit 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 96

Identitätstypen von Personen

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

Tabelle 38: Identitätstypen

Wert	Beschreibung
Primäre Identität	Standardidentität für eine Person. Die Person besitzt ein Standard-benutzerkonto.
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	Virtuelle Person (Subidentität), die ein Benutzerkonto vom Typ

Wert	Beschreibung
Administratoridentität	**Persönliche Administratoridentität** besitzt. Erfassen Sie zusätzlich eine Hauptidentität.
Zusatzidentität	Dummy-Person, die mit einem Benutzerkonto vom Typ **Zusatzidentität** verbunden ist. Weisen Sie der Person einen Manager zu.
Gruppenidentität	Dummy-Person, die mit einem administrativen Benutzerkonto vom Typ **Gruppenidentität** verbunden ist. Weisen Sie der Person einen Manager zu.
Dienstidentität	Dummy-Person, die mit einem Benutzerkonto vom Typ **Dienstidentität** verbunden ist. Weisen Sie der Person einen Manager zu.
Maschinenidentität	Dummy-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 Dummy-Personen dar, über welche die verbundenen Benutzerkonten mit den Berechtigungen in den jeweiligen Zielsystemen versorgt werden. Durch die Einordnung der Dummy-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 Dummy-Personen auslösen. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob Dummy-Personen gesondert betrachtet werden müssen.

Verwandte Themen

- Sonstige Personenstammdaten auf Seite 89
- Abbildung mehrerer Identitäten einer Person auf Seite 95

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.

Folgende Verfahren sind in der Standardinstallation des One Identity Manager verfügbar:

- Zeitweilige Deaktivierung einer Person
- Dauerhafte Deaktivierung einer Person
- Verzögertes Löschen von Personen

Zeitweilige Deaktivierung einer Person

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 einer Person auf Seite 98
- Verzögertes Löschen von Personen auf Seite 100

Dauerhafte Deaktivierung einer Person

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**.

  HINWEIS: 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 einer Person auf Seite 98
- Verzögertes Löschen von Personen auf Seite 100
- Person erneut aktivieren auf Seite 99
- Zertifizierungsstatus einer Person ändern auf Seite 114

Person 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 einer Person auf Seite 98

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. 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.

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`.

Verwandte Themen

- Zeitweilige Deaktivierung einer Person auf Seite 98
- Dauerhafte Deaktivierung einer Person auf Seite 98

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.

HINWEIS: 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>'
```

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 101
- Anwenden einer Kennwortrichtlinie auf Seite 102
- Bearbeiten von Kennwortrichtlinien auf Seite 105
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 108
- Ausschlussliste für Kennwörter festlegen auf Seite 111
- Prüfen eines Kennwortes auf Seite 111
- Generieren eines Kennwortes testen auf Seite 112
- Personen über ablaufende Kennwörter informieren auf Seite 112

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

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 93

Anwenden einer Kennwortrichtlinie

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 101
- Kennwortrichtlinie für die Kennwortspalten ändern auf Seite 103
- Kennwortrichtlinien an Abteilungen, Kostenstellen, Standorte und Geschäftsrollen zuweisen auf Seite 104

Kennwortrichtlinie für die 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 der 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.

Tabelle 39: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. ***Um den Anwendungsbereich festzulegen*** a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** die Tabelle, die die Basisobjekte enthält. Zur Auswahl stehen: • Abteilungen (Tabelle `Department`) • Geschäftsrollen (Tabelle `Org`) HINWEIS: Diese Tabelle steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist. • Standorte (Tabelle `Locality`) • Kostenstellen (Tabelle `Profitcenter`) c. Wählen Sie unter **Anwenden auf** die konkrete Abteilung, Kostenstelle, den Standort oder die Geschäfts-

Eigenschaft	Beschreibung
	rolle. d. 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.

Bearbeiten von Kennwortrichtlinien

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 und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 105
- Richtlinieneinstellungen auf Seite 106
- Zeichenklassen für Kennwörter auf Seite 107
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 108

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 40: Stammdaten einer Kennwortrichtlinie

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

Richtlinieneinstellungen

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

Tabelle 41: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Erstellen eines Benutzerkontos kein Kennwort angegeben oder kein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Wird nur berücksichtigt, bei Anmeldung am One Identity Manager.

Eigenschaft	Bedeutung
	Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen erreicht, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert.
Min. Kennwortstärke	Angabe, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Angabe, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

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

Tabelle 42: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Min. Anzahl	Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens

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

Kundenspezifische Skripte für Kennwortanforderungen

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

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 109
- Skript zum Generieren eines Kennwortes auf Seite 110

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

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

Beispiel für ein Skript zum Prüfen eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **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 110

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

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

Beispiel für ein Skript zum Generieren eines Kennwortes

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

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

```
                spwd.SetAt(0, CChar("_"))
            End If
        End If
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **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 109

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.

Prüfen eines Kennwortes

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

berücksichtigt.

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **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 eines Kennwortes testen

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

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **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 eine Person darüber zu informieren, dass ihr 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 erreicht, 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 Anwenderhandbuch für das Web Portal* und im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Verwandte Themen

- Zentrales Kennwort einer Person auf Seite 93

Eingeschränkter Zugang zum One Identity Manager

HINWEIS: Diese Funktion ist verfügbar, wenn das Modul Attestierung vorhanden ist.

Über das Web Portal können sich Benutzer anmelden, die nur zeitweilig oder mit eingeschränkten Rechten 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 Bearbeitungsrechte 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 einer Person ändern auf Seite 114

Zertifizierungsstatus einer Person ändern

HINWEIS: Diese Funktion ist verfügbar, 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 in 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 113
- Dauerhafte Deaktivierung einer Person auf Seite 98

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 43: 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 in die Gruppen kundendefinierter Zielsysteme aufgenommen.
Active Directory Gruppen	-	+	Alle Active Directory Benutzerkonten und Active Directory Kontakte der Person, für welche die Vererbung von Gruppen zugelassen ist, werden in die Active Directory Gruppen aufgenommen.

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
SharePoint Gruppen	-	+	Alle SharePoint Benutzerkonten der Person werden in die SharePoint Gruppen aufgenommen.
SharePoint Rollen	-	+	Alle SharePoint Benutzerkonten der Person 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 werden in die Notes Gruppen aufgenommen.
SAP Gruppen	+	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen, werden in die SAP Gruppen aufgenommen.
SAP Profile	+	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen, werden in die SAP Profile aufgenommen.
SAP Rollen	+	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen, werden in die SAP Rollen aufgenommen.
Strukturelle Profile	-	+	Alle SAP Benutzerkonten der Person, die im selben SAP Mandanten liegen, werden in die strukturellen Profile aufgenommen.
BI Analyseberechtigungen	-	+	Alle BI Benutzerkonten der Person, die im selben System liegen, erhalten die BI Analyseberechtigungen.
E-Business Suite	-	+	Alle E-Business Suite

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
Berechtigungen			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 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 zugelas-

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkung
			sen ist, werden in die PAM Benutzergruppen aufgenommen.

Detaillierte Informationen zum Thema

- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 24
- Personen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 119
- Personen an Geschäftsrollen zuweisen auf Seite 120
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Arbeiten mit dynamischen Rollen auf Seite 66

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 115
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Arbeiten mit dynamischen Rollen auf Seite 66
- Personen in Kundenknoten des IT Shops aufnehmen auf Seite 121
- Personen an Geschäftsrollen zuweisen auf Seite 120
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53

Personen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion ist verfügbar, 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. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um 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 115

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 Bearbeitungsrechte der Rechtegruppe, 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 werden die Personen der übergeordneten Anwendungsrollen vererbt.

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.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Anwendungsrollen.
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, Standorten 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.

   - ODER -

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

Verwandte Themen

- Ressourcen direkt an Personen zuweisen auf Seite 178
- Ressourcen verwalten auf Seite 172

Software direkt an Personen zuweisen

HINWEIS: Diese Funktion ist verfügbar, 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.

   - ODER -

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

Systemrollen direkt an eine Person zuweisen

HINWEIS: Diese Funktion ist verfügbar, 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 ist verfügbar, 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 zum 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 einer Person 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.

Um die Herkunft von Berechtigungen für eine Person anzuzeigen

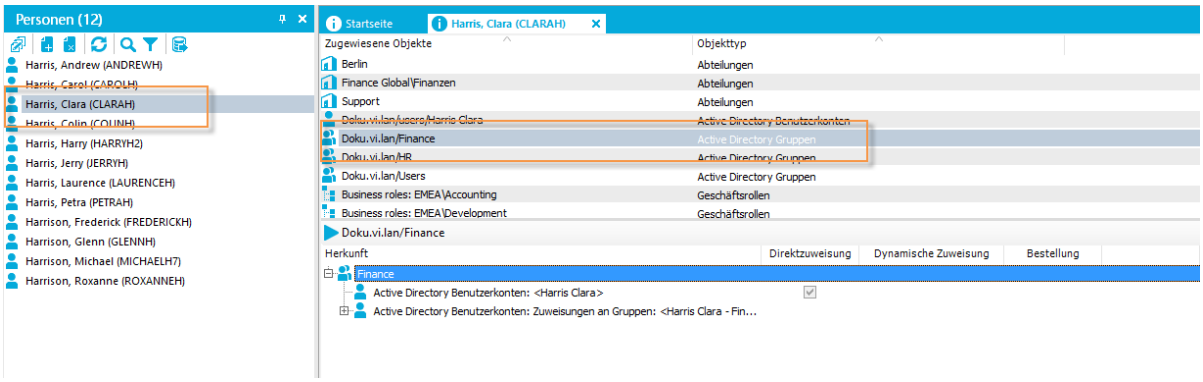
1. Wählen Sie im Manager die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste eine Person aus und führen Sie den Bericht **Herkunft von Berechtigungen anzeigen** aus.
3. Im Bereich **Zugewiesene Objekte** sehen Sie die Berechtigungen, Abteilungen, Kostenstellen, Standorte und Geschäftsrollen 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 zur Herkunft einer Berechtigung

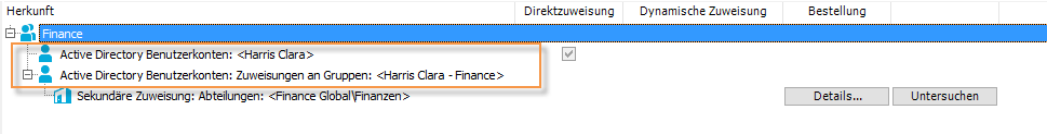
Im Bericht **Herkunft von Berechtigungen anzeigen** wird ermittelt, dass Clara Harris der Active Directory Gruppe "Finance" zugewiesen ist.



Der Bericht beantwortet verschiedene Fragen.

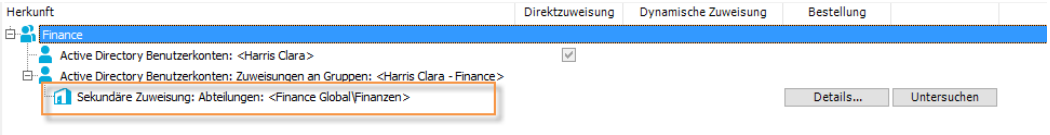
Frage Warum hat Clara Harris die Active Directory Gruppe "Finance"?

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

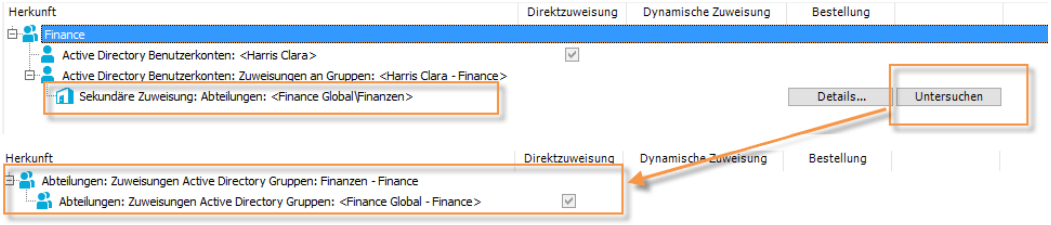


Frage Warum ist dem Benutzerkonto die Gruppe "Finance" zugewiesen?

Antwort Clara Harris ist der Abteilung "Finanzen " zugewiesen.

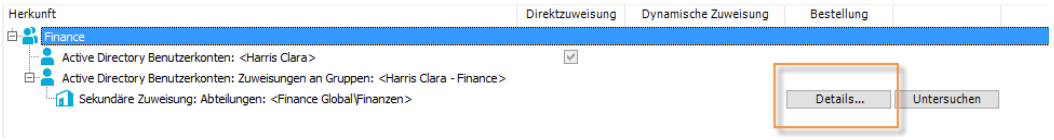


Die Abteilung "Finanzen" erbt von der Abteilung "Finance Global". Der Abteilung "Finance Global" ist die Gruppe "Finance" direkt zugewiesen.



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 44: 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.

Zusätzliche Aufgaben für die Verwaltung von Personen

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

Überblick über eine Person

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.

Benutzerkonten manuell an eine Person 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 eine Person auf Seite 128

Calls für eine Person erfassen

HINWEIS: Diese Funktion ist verfügbar, 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 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 bearbeiten auf Seite 188

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 Anwenderhandbuch für das Web Portal*. 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.

Kennwortfragen festlegen

Falls Sie Ihr Kennwort vergessen, können Sie es jederzeit im Kennwortrücksetzungsportal ändern. Dafür müssen Sie individuelle Fragen hinterlegen, die nur Sie beantworten können.

Die Kennwortfragen legen Sie im Web Portal fest. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

In Ausnahmefällen können Sie die Kennwortabfragen im Manager festlegen.

Um Ihre Kennwortfragen zu erfassen

1. Öffnen Sie im Manager Ihre eigenen Personenstammdaten.
2. Wählen Sie die Aufgabe **Kennwortabfrage ändern**.
3. Auf dem Formular **Kennwortabfragen bearbeiten** klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen:
   - **Frage für Kennwort**: Erfassen Sie Ihre Frage.
   - **Antwort für Kennwort**: Erfassen Sie die Antwort auf Ihre (obige) Frage.
4. Führen Sie die vorherigen Schritte ebenfalls für die restlichen Kennwortfragen aus.
5. Klicken Sie **OK**.

Verwandte Themen

- Nachbarschaftshilfe auf Seite 132

Nachbarschaftshilfe

Um Ihre Kennwörter zu ändern, verwenden Sie das Kennwortrücksetzungsportal. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

In Ausnahmefällen kann eine Person über die Nachbarschaftshilfe im Manager ihr zentrales Kennwort und ihr Systembenutzerkennwort zurücksetzen. Dafür müssen die Kennwortfragen beantwortet werden.

Um Nachbarschaftshilfe zu gewähren

1. Öffnen Sie im Manager Ihre eigenen Personenstammdaten.
2. Wählen Sie die Aufgabe **Nachbarschaftshilfe Kennwortvergabe**.

Die Person, für die Sie Nachbarschaftshilfe gewähren, kann auf diesem Formular ihr zentrales Kennwort und ihr Systembenutzerkennwort ändern.

Um Ihr zentrales Kennwort zu ändern

1. Tragen Sie unter **Anmeldename** Ihr zentrales Benutzerkonto ein.
2. Tragen Sie Ihre Personalnummer ein.
3. Klicken Sie **Weiter**.

   Die Kennwortfragen werden angezeigt.
4. Geben Sie in den Eingabefeldern die entsprechenden Antworten auf Ihre Kennwortfragen ein.
5. Klicken Sie **Freischalten**.
6. Im Eingabefeld **Zentrales Kennwort** geben Sie ein neues Kennwort ein.
7. Im Eingabefeld **Bestätigung** geben Sie das Kennwort erneut ein.
8. Klicken Sie **Speichern**.

Um Ihr Systembenutzerkennwort zu ändern

1. Tragen Sie unter **Anmeldename** Ihr zentrales Benutzerkonto ein.
2. Tragen Sie Ihre Personalnummer ein.
3. Klicken Sie **Weiter**.

   Die Kennwortfragen werden angezeigt.
4. Geben Sie in den Eingabefeldern die entsprechenden Antworten auf Ihre Kennwortfragen ein.
5. Klicken Sie **Freischalten**.
6. Im Eingabefeld **Systembenutzerkennwort** geben Sie ein neues Kennwort ein.
7. Im Eingabefeld **Bestätigung** geben Sie das Kennwort erneut ein.
8. Klicken Sie **Speichern**.

Verwandte Themen

- Kennwortfragen festlegen auf Seite 131

Ermitteln der Sprache einer Person

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 Sprachkultur 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 Arbeitszeit einer Person

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 und der primären Kostenstelle 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 USA.

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 45: 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 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 welche 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 offenen 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**.

Verwandte Themen

- Herkunft von Rollen und Berechtigungen einer Person anzeigen auf Seite 125
- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 127

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.

Detaillierte Informationen zum Thema

- Basisdaten für die Geräteverwaltung auf Seite 137
- Einrichten eines Gerätes auf Seite 145
- Einrichten von Arbeitsplätzen auf Seite 155
- Anlageinformationen für Geräte auf Seite 165

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 auf Seite 138
- Partnerfirmen auf Seite 141
- Gerätestatus auf Seite 142
- Arbeitsplatzstatus auf Seite 143
- Arbeitsplatztypen auf Seite 144
- Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen auf Seite 198

Gerätemodelle

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 bearbeiten

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

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Gerätemodells auf Seite 139
- Inventurdaten eines Gerätemodells auf Seite 140

Allgemeine Stammdaten eines Gerätemodells

Für ein Gerätemodell erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 46: 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 auf Seite 141. 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.
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 Aufgabe **Browsen** wird die angegebene Herstellerseite im Standardwebbrowser angezeigt.

Eigenschaft	Beschreibung
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Zusätzliche Daten	Freitextfeld für zusätzliche Erläuterungen.
PC	Angabe, ob das Gerät prinzipiell als PC im Sinne einer Arbeitsstation einsetzbar ist.
Server	Angabe, ob das Gerät als Server eingesetzt werden soll.
Lokaler Peripherie	Angabe, ob es sich bei diesem Gerätetyp um eine an einen PC anschließbare lokale Peripherie handelt.
Deaktiviert	Angabe, 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 eines Gerätemodells

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 kundenspezifisch angepasst werden.

Tabelle 47: Inventurdaten für ein Gerätemodell

Eigenschaft	Beschreibung
Standard-Lieferant	Lieferantenfirma. Weitere Informationen finden Sie unter Partnerfirmen auf Seite 141.
Person	Person, die für den Kauf zuständig ist.
Alternatives Gerätemodell	Alternatives Gerätemodell.
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.

Eigenschaft	Beschreibung
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

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

Um die Stammdaten für eine Partnerfirma zu bearbeiten

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

   - 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 48: 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.

Eigenschaft	Beschreibung
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 49: 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 **Browsen** wird die angegebene Webseite im Standardwebbrowser angezeigt.

Gerätestatus

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

Um einen Gerätestatus zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Basisdaten zur Konfiguration | Gerätestatus**.
2. Wählen Sie in der Ergebnisliste einen Gerätestatus aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 50: Stammdaten eines Gerätestatus

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

Arbeitsplatzstatus

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

Um einen Arbeitsplatzstatus zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Basisdaten zur Konfiguration | Arbeitsplatzstatus**.
2. Wählen Sie in der Ergebnisliste einen Arbeitsplatzstatus aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 51: Stammdaten eines Arbeitsplatzstatus

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

Arbeitsplatztypen

Zur weiteren Klassifizierung von Arbeitsplätzen erfassen Sie Arbeitsplatztypen. Erfassen Sie zusätzliche Gerätevoraussetzungen, wie beispielsweise die Notwendigkeit von Disketten oder CD-Laufwerken.

Um einen Arbeitsplatztyp zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Basisdaten zur Konfiguration | Arbeitsplatztyp**.
2. Wählen Sie in der Ergebnisliste einen Arbeitsplatztyp aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 52: Stammdaten eines Arbeitsplatztyp

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

Einrichten eines Gerätes

Tabelle 53: 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 bearbeiten

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

- Tablets
- Drucker
- 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 aus.Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Gerätes auf Seite 146
- Netzwerkinformationen für ein Gerät auf Seite 149
- Anlageinformationen für Geräte auf Seite 165
- Unternehmensressourcen an Geräte zuweisen auf Seite 150

Allgemeine Stammdaten eines Gerätes

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

Tabelle 54: Allgemeine Stammdaten eines Gerätes

Eigenschaft	Beschreibung
Anlagegut Nummer	Nummer des Anlagegutes in der Anlagenbuchhaltung.
Gerätekennung	Eindeutige Kennung des Gerätes.
PC	Angabe, ob es sich um einen Computer handelt.
Server	Angabe, ob es sich um einen Server handelt.
Lokale Peripherie	Angabe, ob es sich um lokale Peripheriegeräte handelt, beispielsweise Monitor, Drucker und ein sonstiges Peripheriegerät.
Hersteller	Herstellerfirma.
Gerätemodell	Bezeichnung des Gerätemodells. Die verfügbaren Stammdaten sind abhängig vom gewählten Gerätemodell.

Eigenschaft	Beschreibung
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 der dieses Gerät verknüpft ist.
VM Client (Option)	Angabe, 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)	Angabe, 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.
Standortbeschreibung	Freitextfeld für zusätzliche Erläuterungen.

Eigenschaft	Beschreibung
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 Betriebs-system	Version des Betriebssystems.
Servicepack Betriebs-system	Bezeichnung des Servicepacks.
Hotfix Betriebs-system	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.
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 horizontal	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 auf Seite 138
- Partnerfirmen auf Seite 141
- Gerätestatus auf Seite 142
- Anlageinformationen für Geräte auf Seite 165
- Investitionen und Investitionsvorhaben erfassen auf Seite 167
- Einrichten von Arbeitsplätzen auf Seite 155
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14
- Einschränken der Vererbung über Rollen auf Seite 28

Netzwerkinformationen für ein Gerät

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

Tabelle 55: Netzwerkinformationen

Eigenschaft	Beschreibung
IP-Adresse (IPv4)	IP Adresse im IPv4 Format.
IP-Adresse (IPv6)	IP Adresse im IPv6 Format.
DHCP benutzen	Angabe, 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	Angabe, 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

Eigenschaft	Beschreibung
	werden kann. Im Normalfall ist die Angabe leer zu lassen.
DNS benutzen	Angabe, ob DNS zur Namensauflösung eingesetzt wird. Ist die Option aktiviert, geben Sie die IP-Adressen des bevorzugten und des alternativen DNS-Servers an.
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	Angabe, 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 Gerät 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 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 14
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 24
- Geräte an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 152

- Geräte an Geschäftsrollen zuweisen
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 159
- Arbeiten mit dynamischen Rollen auf Seite 66

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 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 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
    - Primäre Kostenstelle
    - Primärer Standort
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Geräte zuweisen auf Seite 150
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Arbeiten mit dynamischen Rollen auf Seite 66
- Personen an Geschäftsrollen zuweisen auf Seite 120
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53

Geräte an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

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.

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

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

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

    Um eine Zuweisung zu entfernen

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

Um ein Gerät an Geschäftsrollen zuzuweisen (primäre Zuweisung)

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie die primäre Geschäftsrolle.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Geräte zuweisen auf Seite 150
- One Identity Manager Administrationshandbuch für Geschäftsrollen

Zusätzliche Aufgaben zur Verwaltung von Geräten

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

Überblick über das Gerät

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

Servicevereinbarungen zuweisen und Calls erfassen

Installierte Module: Helpdeskmodul

Über das Helpdeskmodul erfassen Sie Servicevereinbarungen und Calls für ein Gerät.

Um Helpdeskdaten für ein Gerät zu erfassen

1. Wählen Sie 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 Lösungs- 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.

Detaillierte Informationen zum Thema

- One Identity Manager Anwenderhandbuch für das Helpdeskmodul

Einrichten von Arbeitsplätzen

Tabelle 57: Konfigurationsparameter für die Einrichtung von Arbeitsplätzen

Konfigurationsparameter	Wirkung bei Aktivierung
Hardware | Workdesk | WorkdeskAuto	Bei Einrichtung einer Arbeitsstation oder eines Servers wird automatisch ein zugehöriger Arbeitsplatz erzeugt.

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 zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Arbeitsplätze | Namen.**
2. Wählen Sie in der Ergebnisliste einen Arbeitsplatz aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Arbeitsplatzes auf Seite 156
- Standortinformationen eines Arbeitsplatzes auf Seite 157
- Sonstige Informationen zu einem Arbeitsplatz auf Seite 158
- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 159
- Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen auf Seite 198

Allgemeine Stammdaten eines Arbeitsplatzes

Erfassen Sie die folgenden allgemeinen Stammdaten zu einem Arbeitsplatz.

Tabelle 58: Allgemeine Stammdaten eines Arbeitsplatzes

Eigenschaft	Beschreibung
Arbeitsplatz	Bezeichnung des Arbeitsplatzes. Ist der Konfigurationsparameter **Hardware | Workdesk | WorkdeskAuto** aktiviert, wird beim Einrichten einer Arbeitsstation oder eines Servers automatisch ein gleich bezeichneter Arbeitsplatz angelegt.
Arbeitsplatztyp	Typ des Arbeitsplatzes.
Status	Status des Arbeitsplatzes.
Betriebssystem	Betriebssystem 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: Die Eigenschaft steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Eigenschaft	Beschreibung
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	Angabe, 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 auf Seite 144
- Arbeitsplatzstatus auf Seite 143
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14
- Einschränken der Vererbung über Rollen auf Seite 28

Standortinformationen eines Arbeitsplatzes

Erfassen Sie die folgenden Informationen zum Standort eines Arbeitsplatzes.

Tabelle 59: 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, dem der Arbeitsplatz primär zugeordnet ist. Bei entsprechender

Eigenschaft	Beschreibung
Standort	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 14

Sonstige Informationen zu einem Arbeitsplatz

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

Tabelle 60: Sonstige Stammdaten eines Arbeitsplatzes

Eigenschaft	Beschreibung
Einrichtungsdatum	Datum der Inbetriebnahme.
Ausmusterung	Datum , zu dem der Arbeitsplatz abgeschrieben ist.
Leasingrate	Leasingrate.
Diskettenlaufwerk notwendig	Angabe, ob an diesem Arbeitsplatz ein Floppylaufwerk benötigt wird.
CD-Laufwerk notwendig	Angabe, 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.

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 61: Mögliche Zuweisungen von Unternehmensressourcen an Arbeitsplätze

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkungen
Systemrollen	+	+	

Unternehmensressource	Direkte Zuweisung möglich	Indirekte Zuweisung möglich	Bemerkungen
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 14
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 26

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen über Rollen auf Seite 24
- Arbeitsplatz an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 160
- Arbeitsplatz an Geschäftsrollen zuweisen
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Arbeiten mit dynamischen Rollen auf Seite 66

Arbeitsplatz 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 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 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
    - Primäre Kostenstelle
    - Primärer Standort
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 159
- Unternehmensressourcen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 54
- Arbeiten mit dynamischen Rollen auf Seite 66
- Geräte an Geschäftsrollen zuweisen auf Seite 153
- Personen, Geräte und Arbeitsplätze an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53

Arbeitsplatz an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

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.

Um einen Arbeitsplatz an Geschäftsrollen zuzuweisen (sekundäre Zuweisung; Standardverfahren)

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Arbeitsplätze | Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um einen Arbeitsplatz an Geschäftsrollen zuzuweisen (primäre Zuweisung)

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Arbeitsplätze | Namen.**
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie die primäre Geschäftsrolle.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Arbeitsplätze zuweisen auf Seite 159
- One Identity Manager Administrationshandbuch für Geschäftsrollen

Software direkt an einen Arbeitsplatz zuweisen

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, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Arbeitsplatz die Software direkt zuweisen. Die Informationen zur Software werden in die Setupdatei der Arbeitsstation geschrieben, die diesem Arbeitsplatz zugewiesen ist.

Um einem Arbeitsplatz Software zuzuweisen

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Arbeitsplätze | Namen**.
2. Wählen Sie in der Ergebnisliste den Arbeitsplatz.
3. Wählen Sie die Aufgabe **Software zuweisen**, um Software an den Arbeitsplatz direkt zuzuweisen.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Software zu.

   - ODER -

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

Verwandte Themen

- Arbeitsplatz an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 160
- Arbeitsplatz an Geschäftsrollen zuweisen auf Seite 162

Systemrollen direkt an einen Arbeitsplatz zuweisen

Installierte Module: Systemrollenmodul

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, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Arbeitsplatz die Systemrollen direkt zuweisen.

Um einem Arbeitsplatz Systemrollen zuzuweisen

1. Wählen Sie 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

- Arbeitsplatz an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 160
- Arbeitsplatz an Geschäftsrollen zuweisen auf Seite 162
- One Identity Manager Administrationshandbuch für Systemrollen

Zusätzliche Aufgaben zur Verwaltung von Arbeitsplätzen

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

Überblick über einen Arbeitsplatz

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 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 den Arbeitsplatz 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 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.

   - ODER -

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

Verwandte Themen

- Allgemeine Stammdaten eines Gerätes auf Seite 146

Personen an einen Arbeitsplatz zuordnen

Nutzen Sie die Aufgabe, um einen Arbeitsplatz an mehrere Personen zuzuweisen. Sie können den Arbeitsplatz auch über die Stammdaten einer Person zuordnen. Durch die Zuordnung eines Arbeitsplatzes an eine Person, wird allen Benutzerkonten dieser Person die zugehörige Arbeitsstation als StammPC zugewiesen. Diese Zuordnung spielt eine Rolle bei der Ermittlung der Applikationslizenzen.

Um Personen an einen Arbeitsplatz zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

Verwandte Themen

- Allgemeine Personenstammdaten auf Seite 83

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.

Detaillierte Informationen zum Thema

- Basisdaten für die Anlagenverwaltung auf Seite 166
- Investitionen und Investitionsvorhaben erfassen auf Seite 167
- Anlageinformationen für ein Gerät bearbeiten auf Seite 168

Basisdaten für die Anlagenverwaltung

Für die Anlagenverwaltung stehen zusätzlich die folgenden Basisdaten zur Verfügung.

- Anlageklassen

  Für die Anlageinformationen zu Geräten erfassen Sie die möglichen Anlageklassen.
- Anlagetypen

  Für die Anlageinformationen zu Geräten erfassen Sie die möglichen Anlagetypen.

Detaillierte Informationen zum Thema

- Anlageklassen auf Seite 166
- Anlagetypen auf Seite 167
- Basisdaten für die Geräteverwaltung auf Seite 137
- Konfigurationsparameter für die Verwaltung von Geräten und Arbeitsplätzen auf Seite 198

Anlageklassen

Erfassen Sie die Anlageklassen für die Anlageinformationen zu einem Gerät.

Um eine Anlageklasse zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Basisdaten zur Konfiguration | Anlageklassen**.
2. Wählen Sie in der Ergebnisliste eine Anlageklasse aus. Wählen Sie die Aufgabe

Stammdaten bearbeiten.

- 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 62: 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

Erfassen Sie die Anlagetypen für die Anlageinformationen zu einem Gerät.

Um einen Anlagetyp zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Basisdaten zur Konfiguration | Anlagetypen**.
2. Wählen Sie in der Ergebnisliste einen Anlagetyp aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 erfassen

Erfassen Sie Angaben zu Investitionen und Investitionsvorhaben und weisen Sie diese an die Geräte zu.

Um eine Investition zu bearbeiten

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | Investitionen**.
2. Wählen Sie in der Ergebnisliste eine Investition aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die folgenden Stammdaten.

   Tabelle 63: 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 eines Gerätes auf Seite 146

Anlageinformationen für ein Gerät bearbeiten

Um die Anlageinformationen für ein Gerät zu erfassen

1. Wählen Sie die Kategorie **Geräte & Arbeitsplätze | <Filter>**.
2. Wählen Sie in der Ergebnisliste das Gerät.
3. Wählen Sie die Aufgabe **Kaufmännische Daten bearbeiten**.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten für die Anlageinformationen auf Seite 169
- Kaufmännische Daten auf Seite 170

Stammdaten für die Anlageinformationen

Erfassen Sie die folgenden Stammdaten für die Anlageinformationen eines Gerätes.

Tabelle 64: 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.
Restbuchwert	Restbuchwert des Gerätes.
Firmeneigentum	Angabe, ob es sich um Eigentum der Firma handelt.
Leasing	Angabe, 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.
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 auf Seite 166
- Anlagetypen auf Seite 167
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14

Kaufmännische Daten

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 kundenspezifisch angepasst werden.

Tabelle 65: Kaufmännische Daten eines Gerätes

Eigenschaft	Beschreibung
Anschaffungsdatum	Datum des Kaufs.
Lieferdatum	Datum der Lieferung.
Lieferscheinnummer	Lieferscheinnummer.
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.
Leasingrate	Leasingrate.
Interner Verrechnungspreis	Interner Verrechnungspreis.
Abschreibungsmonat	Abschreibungsdauer in Monaten.

Verwandte Themen

- Partnerfirmen auf Seite 141

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 66: 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 zurückgegeben werden müssen, wenn sie nicht mehr benötigt werden. Nach Genehmigung werden die Ressourcen an die Personen zugewiesen. Sie bleiben so lange zugewiesen, bis sie abbestellt werden. Beispiele: Drucker, Monitor	QERReuseUS

Detaillierte Informationen zum Thema

- Ressourcen bearbeiten auf Seite 174
- Ressourcen an Personen zuweisen auf Seite 176
- Mehrfach bestellbare Ressourcen bearbeiten auf Seite 181
- Mehrfach bestellbare Ressourcen an Personen zuweisen auf Seite 183
- Berichte über Ressourcen auf Seite 185

One Identity Manager Benutzer für die Verwaltung von Ressourcen

In die Verwaltung von Ressourcen sind folgende Benutzer eingebunden.

Tabelle 67: 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 und Personen zu.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • 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 174
- Zusatzeigenschaften bearbeiten auf Seite 188

Ressourcentypen

Ressourcentypen können zur Gruppierung von Ressourcen genutzt werden.

Um Ressourcentypen zu definieren

1. Wählen Sie die Kategorie **Berechtigungen | Basisdaten zur Konfiguration | Ressourcentypen**.
2. Wählen Sie in der Ergebnisliste einen Ressourcentyp aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   – ODER –

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie eine Bezeichnung und eine Beschreibung für den Ressourcentyp.
4. Speichern Sie die Änderungen.

Ressourcen bearbeiten

Um Ressourcen zu bearbeiten

1. Wählen Sie die Kategorie **Berechtigungen | Ressourcen**.
2. Wählen Sie in der Ergebnisliste eine Ressource aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Stammdaten einer Ressource auf Seite 175
- Ressourcen an Personen zuweisen auf Seite 176

Stammdaten einer Ressource

Für eine Ressource erfassen Sie folgende allgemeine Stammdaten.

Tabelle 68: Stammdaten einer Ressource

Eigenschaft	Beschreibung
Ressource	Bezeichnung der 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.
Vorausgesetzte Ressource	Definieren Sie Abhängigkeiten zwischen Ressourcen. Wenn die Ressource bestellt oder zugeordnet wird, wird die vorausgesetzte Ressource automatisch mitbestellt oder zugeordnet.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Ressource an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist.
IT Shop	Angabe, 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.
Verwendung nur im IT Shop	Angabe, ob die Ressource ausschließlich über den IT Shop bestellbar ist. Die Ressource kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Ressource an Rollen außerhalb des IT Shop ist nicht zulässig.
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.

Eigenschaft	Beschreibung
Automatische Zuweisung an Personen	Angabe, 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 Person neu angelegt wird, erhält sie 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 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 174
- One Identity Manager Administrationshandbuch für Risikobewertungen
- One Identity Manager Administrationshandbuch für IT Shop

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 sind

- 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 erlauben auf Seite 26
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14

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 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 verwalten auf Seite 31
- Grundlagen zur Abbildung von Unternehmensstrukturen im One Identity Manager auf Seite 9

Ressourcen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie eine Ressource an Geschäftsrollen zu, damit die Ressource über diese Geschäftsrollen an Personen vererbt wird.

Um eine Ressource an Geschäftsrollen zuzuweisen

1. Wählen Sie die Kategorie **Berechtigungen | Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für Geschäftsrollen

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, Standorten 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 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 73
- Grundlagen zur Zuweisung von Unternehmensressourcen auf Seite 14

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.

Um eine Ressource in den IT Shop aufzunehmen

1. Wählen Sie 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 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 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 einer Ressource auf Seite 175
- One Identity Manager Administrationshandbuch für IT Shop

Ressourcen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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.

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 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.

   - ODER -

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

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für Systemrollen

Zusätzliche Aufgaben für die Verwaltung von Ressourcen

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

Überblick über eine Ressource

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 die Kategorie **Berechtigungen | Ressourcen**.
2. Wählen Sie in der Ergebnisliste die Ressource.
3. Wählen Sie die Aufgabe **Überblick über die Ressource**.

Zusatzeigenschaften an eine Ressource 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 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.

   - ODER -

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

Detaillierte Informationen zum Thema

- Zusatzeigenschaften bearbeiten auf Seite 188

Mehrfach bestellbare Ressourcen 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 bearbeiten

1. Wählen Sie die Kategorie **Berechtigungen | Mehrfach bestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste eine Ressource aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 bearbeiten

1. Wählen Sie die Kategorie **Berechtigungen | Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
2. Wählen Sie in der Ergebnisliste eine Ressource aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 einer mehrfach bestellbaren Ressource auf Seite 182
- Mehrfach bestellbare Ressourcen an Personen zuweisen auf Seite 183

Stammdaten einer mehrfach bestellbaren Ressource

Für eine mehrfach bestellbare Ressource erfassen Sie folgende allgemeine Stammdaten.

Tabelle 69: Stammdaten einer mehrfach bestellbaren Ressource

Eigenschaft	Beschreibung
Mehrfach bestellbare Ressource	Bezeichnung der Ressource.
Mehrfach zu-	

Eigenschaft	Beschreibung
/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. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist.
IT Shop	Angabe, 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.
Verwendung nur im IT Shop	Angabe, ob die Ressource ausschließlich über den IT Shop bestellbar ist. Die Ressource kann über das Web Portal von den 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.
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 174
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für Risikobewertungen

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.

Detaillierte Informationen zum Thema

- Zuweisung über IT Shop Bestellungen auf Seite 18
- One Identity Manager Administrationshandbuch für IT Shop

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.

Um eine mehrfach bestellbare Ressource in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **Berechtigungen | Mehrfach bestellbare Ressourcen für IT Shop**.

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
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 mehrfach bestellbare Ressource aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Berechtigungen | Mehrfach bestellbare Ressourcen für IT Shop**.

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Mehrfach zu-/abbestellbare Ressourcen für IT Shop**.
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 mehrfach bestellbare Ressource aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Berechtigungen | Mehrfach bestellbare Ressourcen für IT Shop**.

   - ODER -

   Wählen Sie 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.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für IT Shop

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 70: 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 127

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 erstellen auf Seite 187
- Zusatzeigenschaften bearbeiten auf Seite 188

One Identity Manager Benutzer für die Verwaltung von Zusatzeigenschaften

In die Verwaltung von Zusatzeigenschaften sind folgende Benutzer eingebunden.

Tabelle 71: 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	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Eigenschaftengruppen 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.

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.

Zusatzeigenschaften 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 einer Zusatzeigenschaft auf Seite 188
- Bereichsgrenzen festlegen auf Seite 189

Stammdaten einer Zusatzeigenschaft

Für eine Zusatzeigenschaft erfassen Sie die folgenden Stammdaten.

Tabelle 72: 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 Navigationsansicht nach dieser Eigenschaftengruppe gruppiert. Sollte die Zuordnung einer Zusatzeigenschaft zu mehreren

Eigenschaft	Beschreibung
	Eigenschaftengruppen notwendig sein, so können Sie über die Aufgabe **Eigenschaftengruppen zuweisen** 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.

Detaillierte Informationen zum Thema

- Bereichsgrenzen festlegen auf Seite 189

Bereichsgrenzen 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*.

Zusätzliche Aufgaben für die Verwaltung von Zusatzeigenschaften

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

Überblick über eine Zusatzeigenschaft

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 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 **Objekttyp auswählen** den gewünschten Objekttyp.

   Es werden die zum Objekttyp gehörigen Objekte auf dem Formular angezeigt.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Objekte zu.

   - ODER -

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

Eigenschaftengruppen zuweisen

Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein.

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.

   - ODER -

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

Verwandte Themen

- Eigenschaftengruppen erstellen auf Seite 187

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 73: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | Structures	Ist der Konfigurationsparameter aktiviert, werden hierarchische Rollen unterstützt.
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. 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

Konfigurationsparameter	Beschreibung
	aktiviert, werden die Berechnungsaufträge beim nächsten Lauf des Zeitplans eingestellt.
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.
QER | Structures | Inherite | Person	Der Konfigurationsparameter legt fest, ob Personen über primäre Zuweisung erben.
QER | Structures | Inherite | Person | FromDepartment	Der Konfigurationsparameter legt fest, ob Personen die Zuordnungen von ihrer primären Abteilung (`Person.UID_Department`) erben.
QER | Structures | Inherite | Person | FromLocality	Der Konfigurationsparameter legt fest, ob Personen die Zuordnungen von ihrem primären Standort (`Person.UID_Locality`) erben.
QER | Structures | Inherite | Person | FromProfitCenter	Der Konfigurationsparameter legt fest, ob Personen die Zuordnungen von ihrer primären Kostenstelle (`Person.UID_ProfitCenter`) erben.
QER | Structures | Inherite | Hardware	Der Konfigurationsparameter legt fest, ob Geräte über primäre Zuweisung erben.
QER | Structures | Inherite | Hardware | FromDepartment	Der Konfigurationsparameter legt fest, ob Geräte die Zuordnungen von ihrer primären Abteilung (`Hardware.UID_Department`) erben.
QER | Structures | Inherite | Hardware | FromLocality	Der Konfigurationsparameter legt fest, ob Geräte die Zuordnungen von ihrem primären Standort (`Hardware.UID_Locality`) erben.
QER | Structures | Inherite | Hardware | FromProfitCenter	Der Konfigurationsparameter legt fest, ob Geräte die Zuordnungen von ihrer primären Kostenstelle (`Hardware.UID_ProfitCenter`) erben.
QER | Structures | Inherite | Workdesk	Der Konfigurationsparameter legt fest, ob Arbeitsplätze über primäre Zuweisung erben.
QER | Structures | Inherite | Workdesk | FromDepartment	Der Konfigurationsparameter legt fest, ob Arbeitsplätze die Zuordnungen von ihrer primären Abteilung (`Workdesk.UID_Department`) erben.
QER | Structures | Inherite | Workdesk | FromLocality	Der Konfigurationsparameter legt fest, ob Arbeitsplätze erben die Zuordnungen von ihrem primären Standort (`Workdesk.UID_Locality`) erben.

Konfigurationsparameter	Beschreibung
QER | Structures | Inherite | Workdesk | FromProfitCenter	Der Konfigurationsparameter 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 74: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | Person	Ist der Konfigurationsparameter aktiviert, wird die Verwaltung von Personen unterstützt.
QER | Person | CentralAccountGlobalUnique	Der Konfigurationsparameter 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 Zielsystemen. Ist der Konfigurationsparameter nicht aktiviert, erfolgt die Bildung nur eindeutig bezogen auf die zentralen Benutzerkonten aller Personen.
QER | Person | DefaultMailDomain	Der Konfigurationsparameter enthält die Standardmaildomäne. Der Wert dient zur Bestimmung der Standard-E-Mail-Adresse einer Person.
Person | MasterIdentity | UseMasterForAuthentication	Der Konfigurationsparameter legt fest, 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 |	Der Konfigurationsparameter legt fest, ob die

Konfigurationsparameter	Beschreibung
PasswordResetAuthenticator | InvalidateUsedQuery	Kennwortfragen, die für eine erfolgreiche Kennwortrücksetzung verwendet wurden, ungültig werden.
QER | Person | PasswordResetAuthenticator | QueryAnswerDefinitions	Der Konfigurationsparameter bestimmt die Anzahl von Kennwortfragen, die eine Person festlegen muss, um ihr Kennwort ändern zu können.
QER | Person | PasswordResetAuthenticator | QueryAnswerRequests	Der Konfigurationsparameter bestimmt die Anzahl von Kennwortfragen, die eine Person beantworten muss, um ihr Kennwort zu ändern.
QER | Person | PasswordResetAuthenticator | PasscodeSplit	Der Konfigurationsparameter legt fest, 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	Der Konfigurationsparameter 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	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort einer Person in den Benutzerkonten verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
QER | Person | UseCentralPassword | CheckAllPolicies	Der Konfigurationsparameter legt fest, 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.
QER | Person | UseCentralPassword | PermanentStore	Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennworte. Ist der Konfigurationsparameter aktiviert, wird das zentrale Kennwort in der One Identity Manager-Datenbank gespeichert und wird für neue Benutzerkonten genutzt. Ist der Konfigurationsparameter deaktiviert, wird das zentrale Kennwort nach dem Publizieren an die bestehenden Benutzerkonten aus der One Identity Manager-Datenbank

Konfigurationsparameter	Beschreibung
	gelöscht werden. Das zentrale Kennwort steht für weitere Benutzerkonten nicht zur Verfügung.
QER | Person | UseCentralPassword | SyncToSystemPassword	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort der Person auf das Systembenutzerkennwort der Person übernommen wird.
QER | Person | UseCentralPassword | SyncToSystemPassword | UnlockByCentralPassword	Der Konfigurationsparameter legt fest, ob das Systembenutzerkonto der Person bei der Synchronisation des zentralen Kennworts auch entsperrt wird.
SysConfig	Ist der Konfigurationsparameter aktiviert, können allgemeine Einstellungen zum Systemverhalten konfiguriert werden.
SysConfig | Display	Ist der Konfigurationsparameter aktiviert, wird die Konfiguration der Frontendgestaltung unterstützt.
SysConfig | Display | SourceDetective	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Anzeige der Herkunft von Berechtigungen einer Person. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

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 75: 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.
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.
Hardware | Display	Der Konfigurationsparameter legt fest, ob die Anzeige von Geräteeigenschaften konfiguriert werden kann.
Hardware | Display | CustomHardwareType	Der Konfigurationsparameter legt fest, ob beim Einrichten eines neuen Gerätes mit dem entsprechenden Gerätemodell auf die Stammdaten angepasste Formulare angezeigt werden.
Hardware | Display | CustomHardwareType | MobilePhone	Der Konfigurationsparameter enthält die Angabe des Gerätetyps, der ein Mobiltelefone repräsentiert.
Hardware | Display | CustomHardwareType | Monitor	Der Konfigurationsparameter enthält die Angabe des Gerätetyps, der einen Monitor repräsentiert.

Konfigurationsparameter	Beschreibung
Hardware | Display | CustomHardwareType | PC	Der Konfigurationsparameter enthält die Angabe des Gerätetyps, der einen PC repräsentiert.
Hardware | Display | CustomHardwareType | Printer	Der Konfigurationsparameter enthält die Angabe des Gerätetyps, der einen Drucker repräsentiert.
Hardware | Display | CustomHardwareType | Server	Der Konfigurationsparameter enthält die Angabe des Gerätetyps, der einen Server repräsentiert.
Hardware | Display | CustomHardwareType | Tablet	Der Konfigurationsparameter enthält die Angabe des Gerätetyps, der ein Tablet repräsentiert.
Hardware | Display | DisplayResolutions	Der Konfigurationsparameter enthält eine Pipe-getrennte Auflistung aller Bildschirmauflösungen, die auf den Stammdatenformularen der Geräte zur Auswahl angeboten werden.
Hardware | Display | MachineWithRPL	Der Konfigurationsparameter 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	Der Konfigurationsparameter legt fest, ob bei Einrichtung einer Arbeitsstation oder eines Servers automatisch ein zugehöriger Arbeitsplatz erzeugt wird.

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

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

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

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

Index

A

B

D

E

G

H

I

K

L

M

N

P

R

S

U

V

Z