One Identity Manager 8.1

Administrationshandbuch für Geschäftsrollen

Legende

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

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

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

One Identity Manager Administrationshandbuch für Geschäftsrollen
Aktualisiert - März 2019
Version - 8.1

Inhalt

Geschäftsrollen verwalten

Geschäftsrollen bilden Unternehmensstrukturen mit gleichartiger Funktionalität ab, die zusätzlich zu Abteilungen, Kostenstellen und Standorten existieren. Das können zum Beispiel Projektgruppen sein. An Geschäftsrollen können verschiedene Unternehmensressourcen zugewiesen werden, beispielsweise Berechtigungen in SAP Systemen oder Applikationen. Personen können als Mitglieder in die einzelnen Geschäftsrollen aufgenommen werden. Bei entsprechender Konfiguration des One Identity Manager erhalten die Personen über diese Zuordnungen ihre Unternehmensressourcen.

Die One Identity Manager Bestandteile für Verwaltung von Geschäftsrollen sind verfügbar, wenn der Konfigurationsparameter "QER/Org" aktiviert ist.

- Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

One Identity Manager Benutzer für Geschäftsrollen

In die Verwaltung von Geschäftsrollen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen und Bearbeiten die Geschäftsrollen. • Weisen Unternehmensressourcen an die Geschäftsrollen zu. • Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer.

Benutzer	Aufgaben
	• 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 Geschäftsrollen	Die Attestierer müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Attestierer** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Geschäftsrollen, für die sie verantwortlich sind. • Können die Stammdaten der Geschäftsrollen sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Grundlagen für den Aufbau von hierarchischen Rollen

Geschäftsrollen 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.

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.

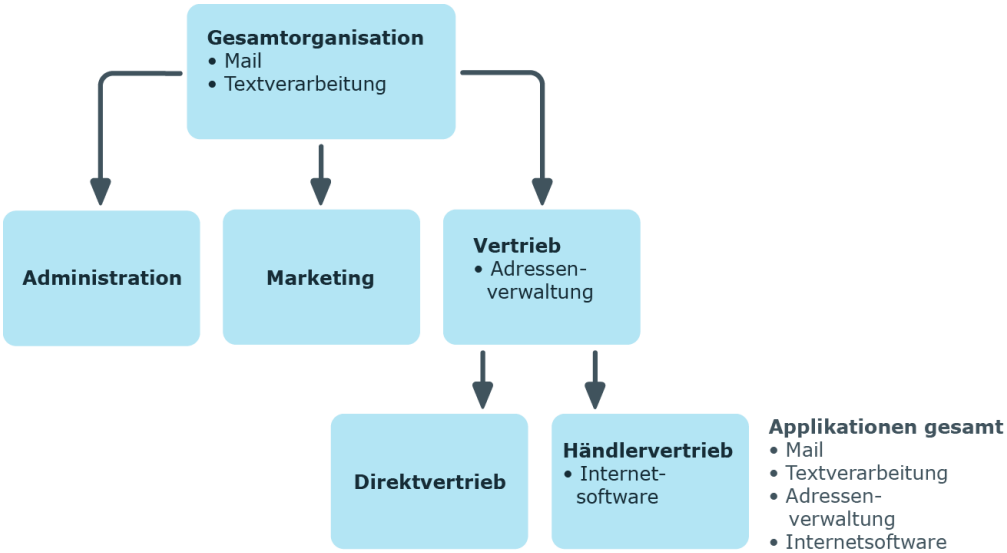
HINWEIS: Die Vererbungsrichtung wird nur bei der Vererbung von Unternehmensressourcen beachtet. Auf die Ermittlung der verantwortlichen Manager hat die Vererbungsrichtung keinen Einfluss. Der Manager einer übergeordneten Rolle ist immer für alle untergeordneten Rollen verantwortlich.

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 der jeweiligen Abteilung zugeordnete Applikationen eingetragen. Eine Person des Händlervertriebes erhält alle Applikationen, die ihrer Abteilung und allen Abteilungen auf dem Pfad zur Gesamtorganisation zugewiesen sind. In diesem Fall sind das die Internetsoftware, Adressenverwaltung, Mail und Textverarbeitung.

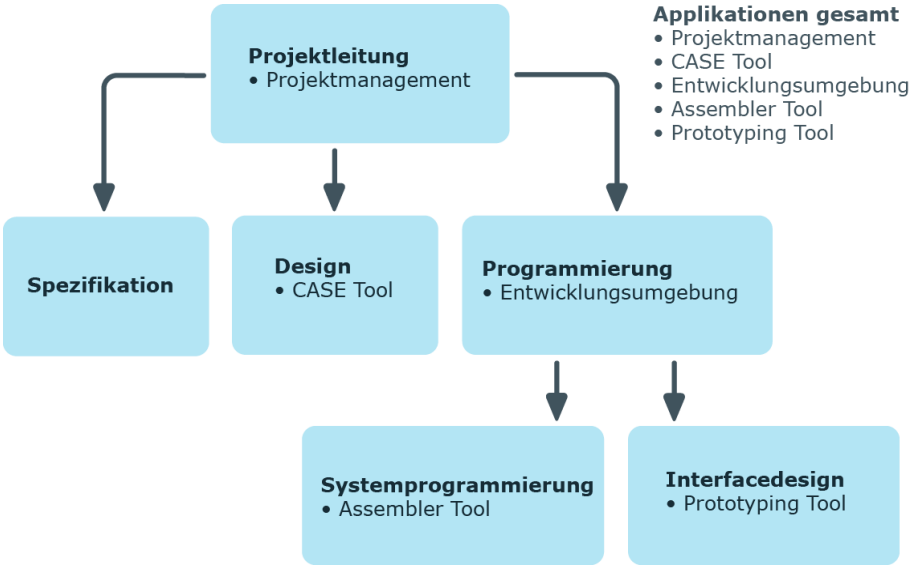
Abbildung 1: Zuweisung über Top-Down-Vererbung



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 der jeweiligen Projektgruppen zugeordnete Applikationen eingetragen. Eine Person der Projektgruppe "Projektleitung" erhält neben den Applikationen ihrer Projektgruppe alle Applikationen 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

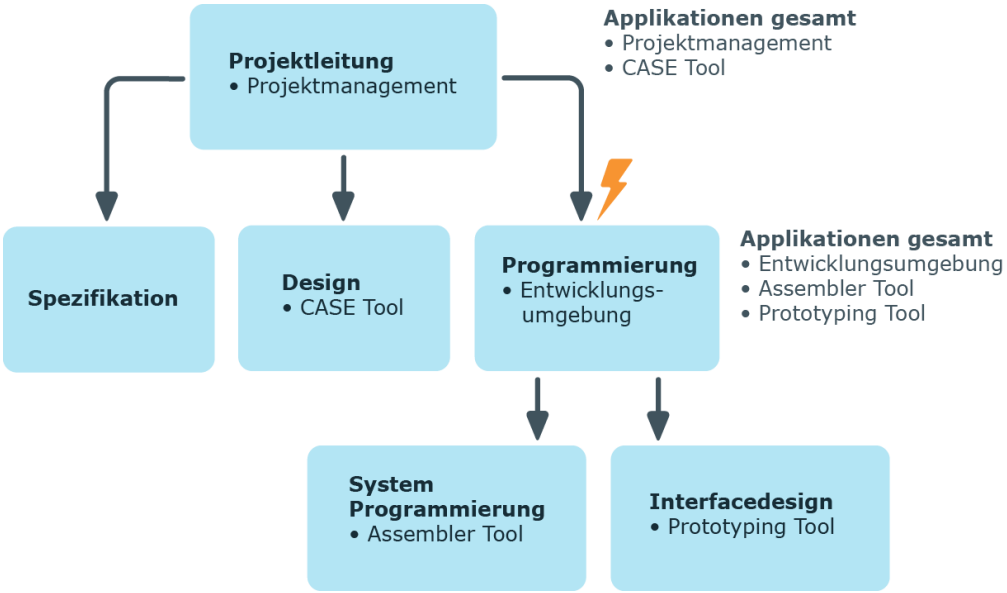
Wird im Beispiel einer Top-Down-Vererbung für die Abteilung "Vertrieb" die Option **Vererbung blockieren** gesetzt, hat das zur Folge, dass eine Person in der Abteilung "Vertrieb" nur die Adressenverwaltung und eine Person in der Abteilung "Händlervertrieb" die Adressenverwaltung und Internetsoftware erbt. Die Applikationen der Abteilung "Gesamtorganisation" werden jedoch nicht an den Vertrieb und den 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 Applikationen seiner Projektgruppe alle Applikationen 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 Applikation Projektmanagement nur das CASE Tool zugewiesen. Die Applikationen 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

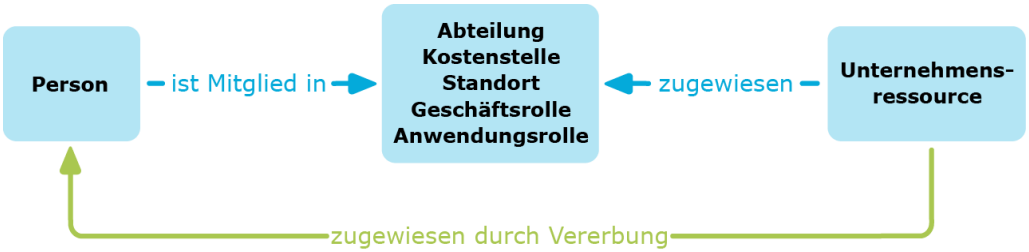
Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Person, einem Gerät oder einem Arbeitsplatz. Durch die direkte Zuweisung von Unternehmensressourcen kann ohne weiteren Aufwand auf Sonderanforderungen reagiert werden.

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.

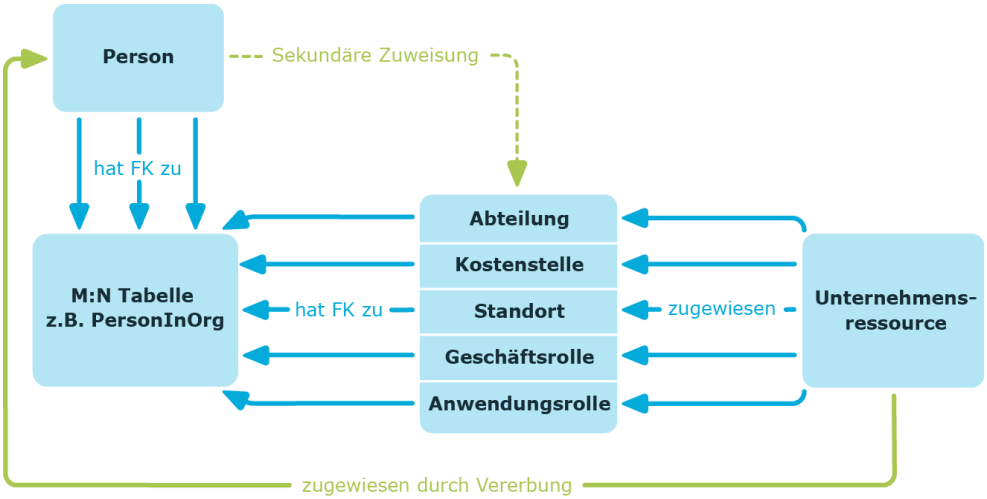
Abbildung 6: Schema einer indirekten Zuweisung am Beispiel Person



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 fest.

Abbildung 7: Schema einer sekundären Zuweisung



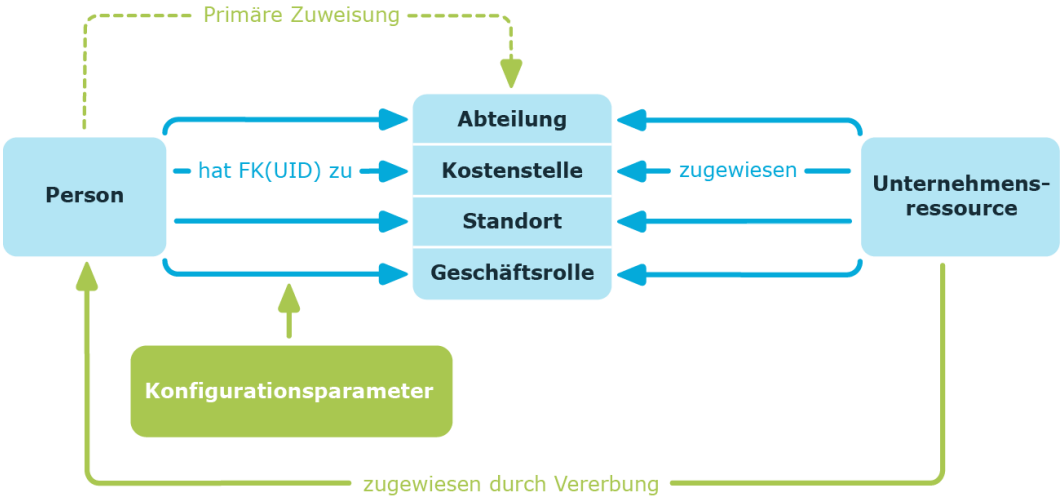
Verwandte Themen

- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 21

Primäre Zuweisung

Die primäre Zuweisung erfolgt über die Fremdschlüssel-Referenzierung einer Geschäftsrolle 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 2: Konfigurationsparameter für die primäre Zuweisung

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | Person	Personen können über primäre Zuweisung erben.
QER | Structures | Inherite | Person | FromOrg	Personen erben die Zuordnungen von ihrer primären Geschäftsrolle (Person.UID_Org).
QER | Structures | Inherite | Hardware	Geräte können über primäre Zuweisung erben.
QER | Structures | Inherite | Hardware | FromOrg	Geräte erben die Zuordnungen von ihrer primären Geschäftsrolle (Hardware.UID_Org).
QER | Structures | Inherite | Workdesk	Arbeitsplätze können über primäre Zuweisung erben.
QER | Structures | Inherite | Workdesk | FromOrg	Arbeitsplätze erben die Zuordnungen von ihrer primären Geschäftsrolle (Workdesk.UID_Org).

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 Geschäftsrolle zugewiesen werden; verlässt eine Person diese Geschäftsrolle 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

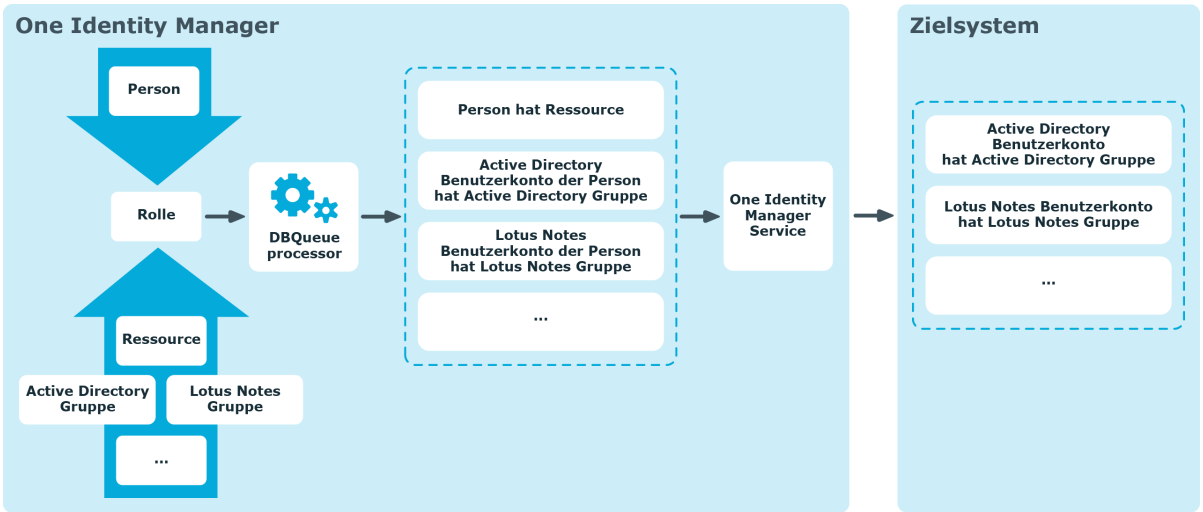
zugewiesen. Neben den Unternehmensressourcen können über den IT Shop auch Rollenmitgliedschaften bestellt werden.

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



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.

Tabelle 3: Sichten auf die Tabelle BaseTree

Sicht	Bedeutung
Org	Abbildung von Geschäftsrollen

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:

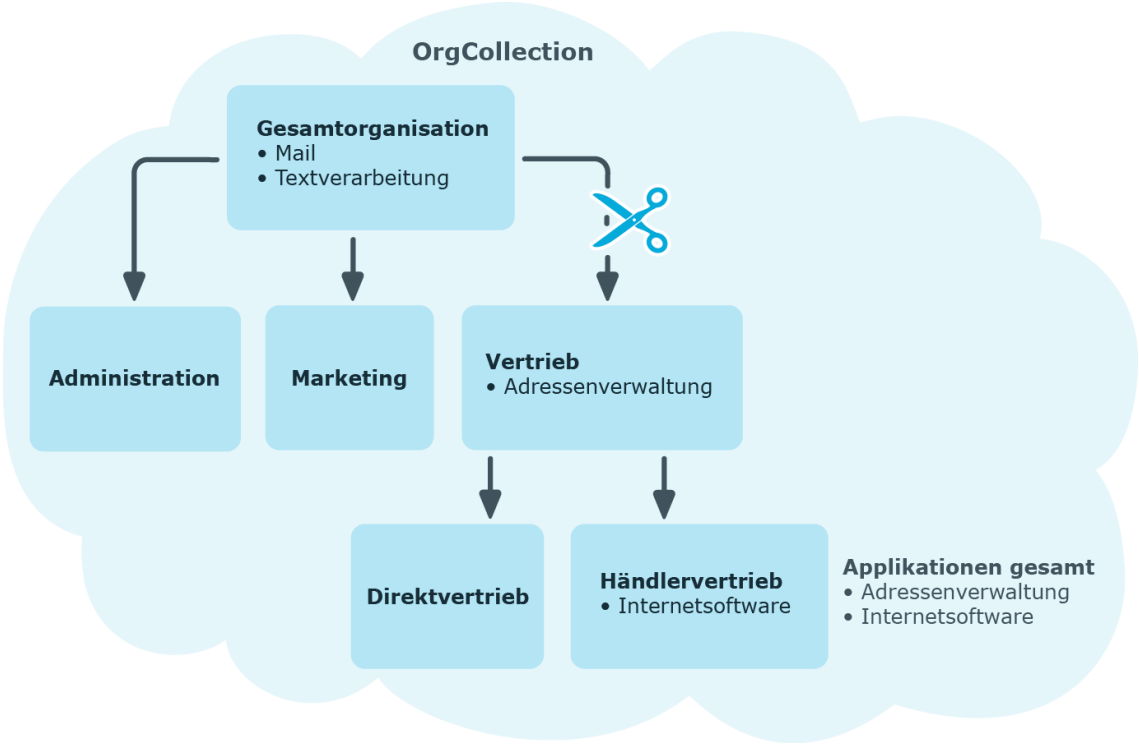
- UID_Org ist die Rolle, die erbt.
- UID_ParentOrg ist die Rolle, die vererbt.

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 eine Applikation 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.

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 4: Mögliche Werte der Spalte XOrigin

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

Bit 3	Bit 2	Bit 1	Bit 0	Wert in XOrigin	Bedeutung
1	1	1	1	**15**	Zuweisungsbestellung, direkt, indirekt und über dynamische Rolle zugewiesen.

Vorbereiten der Geschäftsrollen für die Zuweisung von Unternehmensressourcen

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.
- Legen Sie die Vererbungsrichtung innerhalb der Hierarchie fest.
- 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

- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 21
- Festlegen der Vererbungsrichtung auf Seite 22
- Einschränken der Vererbung über Geschäftsrollen auf Seite 22
- Vererbungsausschluss für Geschäftsrollen festlegen auf Seite 48

Mögliche Zuweisungen von Unternehmensressourcen

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 5: 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)	-
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)	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Personen	Arbeitsplätze
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)	-
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	-
Applikationen	möglich	möglich

Verwandte Themen

- Unternehmensressourcen an Geschäftsrollen zuweisen auf Seite 37

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.

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 Geschäftsrollen zuzuweisen, aktivieren Sie an der Rollenklasse "Geschäftsrolle", für den Eintrag "Personen", die Optionen **Zuweisungen erlaubt** und **Direkte Zuweisungen erlaubt**.

Sollen Personen die Mitgliedschaft in einer Geschäftsrolle nur über den IT Shop erhalten, dann aktivieren Sie an der Rollenklasse "Geschäftsrolle", 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.

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.

Festlegen der Vererbungsrichtung

Innerhalb einer Rollenhierarchie entscheidet die Vererbungsrichtung über die Zuteilung der Unternehmensressourcen. Die Vererbungsrichtung wird an den Rollenklassen festgelegt.

Die Vererbungsrichtung kann nur beim Einfügen einer Rollenklasse festgelegt werden.

- Um die Top-Down-Vererbung festzulegen, aktivieren Sie die Option **Vererbt von oben nach unten**.
- Um die Bottom-Up-Vererbung festzulegen, aktivieren Sie die Option **Vererbt von unten nach oben**.

Detaillierte Informationen zum Thema

- Vererbungsrichtungen innerhalb einer Hierarchie auf Seite 7
- Rollenklassen auf Seite 27

Einschränken der Vererbung über Geschäftsrollen

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 die Option
   - **Keine Vererbung an Personen**
   - **Keine Vererbung an Geräte**

     - ODER -
   - **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 9

Vererbungsausschluss: Festlegen widersprechender Rollen

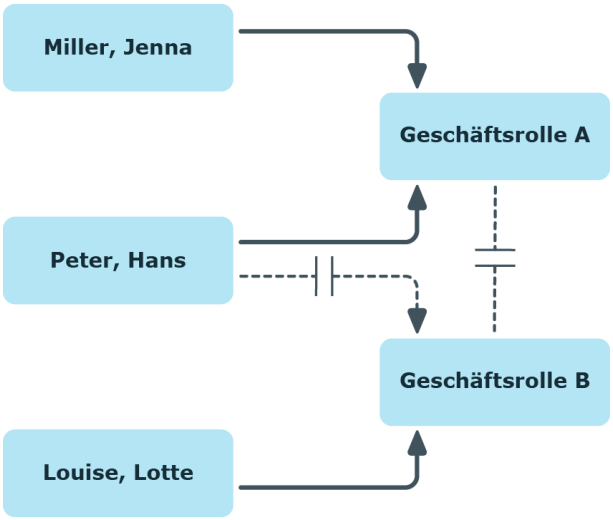
Um zu verhindern, dass Personen, Geräte oder Arbeitsplätze gleichzeitig an verschiedene Rollen zugewiesen werden und über diese Rollen sich ausschließende Unternehmensressourcen erhalten könnten, können Sie widersprechende Rollen definieren. Dabei legen Sie fest, welche Geschäftsrollen sich gegenseitig 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 Geschäftsrolle A wurde Geschäftsrolle B als widersprechende Geschäftsrolle eingetragen. Jenna Miller und Hans Peter sind Mitglied der Geschäftsrolle A. Lotte Louise ist Mitglied der Geschäftsrolle B. Hans Peter kann nicht an Geschäftsrolle B zugewiesen werden. Der One Identity Manager verhindert außerdem, dass Jenna Miller an Geschäftsrolle B und Lotte Louise an Geschäftsrolle 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 Geschäftsrollen festlegen auf Seite 48

Basisdaten zum Aufbau von Geschäftsrollen

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 Geschäftsrollen Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows für die Attestierungsvorgänge als verantwortliche Attestierer herangezogen werden. Dazu ordnen Sie den Geschäftsrollen 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 Geschäftsrollen Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows als verantwortliche Entscheider für Genehmigungsverfahren bei IT Shop-Bestellungen herangezogen werden. Dazu ordnen Sie den Geschäftsrollen die 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 27
- Rollentypen auf Seite 28
- Unternehmensbereiche auf Seite 28
- Attestierer auf Seite 30
- Genehmiger und Genehmiger (IT) auf Seite 31

Rollenklassen

Geschäftsrollen werden in der Navigationsansicht nach Rollenklassen gruppiert. Jede Geschäftsrolle ist genau einer Rollenklasse zugeordnet. Bevor Sie Geschäftsrollen anlegen können, definieren Sie dafür geeignete Rollenklassen.

Um Rollenklassen zu bearbeiten

1. Wählen Sie die Kategorie **Geschäftsrollen | Basisdaten zur Konfiguration | Rollenklassen**.
2. Wählen Sie in der Ergebnisliste eine Rollenklasse aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Für eine Rollenklasse erfassen Sie die folgenden Stammdaten.

Tabelle 6: Eigenschaften von Rollenklassen

Eigenschaft	Beschreibung
Rollenklasse	Bezeichnung der Rollenklasse. Unter dieser Bezeichnung wird die Rollenklasse in der Navigationsansicht angezeigt.
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge für alle Rollen dieser Rollenklasse 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.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Vererbt von oben nach unten	Vererbungsrichtung Top-Down.
Vererbt von unten nach oben	Vererbungsrichtung Bottom-Up.
Delegierbar	Angabe, ob die Mitgliedschaften in den Rollen dieser Rollenklasse delegiert werden können.
Zuweisungen	Angabe, ob die Zuweisung der jeweiligen Objekttypen zu Rollen der

Eigenschaft	Beschreibung
erlaubt	Rollenklasse generell erlaubt ist.
Direkte Zuweisungen erlaubt	Angabe, ob die jeweiligen Objekttypen direkt an die Rollen der Rollenklasse zugewiesen werden kann.

Verwandte Themen

- Vererbungsrichtungen innerhalb einer Hierarchie auf Seite 7
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 21

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 **Geschäftsrollen | 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 7: 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 Geschäftsrollen soll bewertet werden. Gehen Sie folgendermaßen vor:

1. Richten Sie Unternehmensbereiche ein.
2. Ordnen Sie die Unternehmensbereiche den Geschäftsrollen zu.
3. Definieren Sie Bewertungskriterien für die Geschäftsrollen.
4. Definieren Sie Bewertungskriterien für die Unternehmensbereiche.
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 die Kategorie **Geschäftsrollen | Basisdaten zur Konfiguration | Unternehmensbereiche**.
2. Wählen Sie in der Ergebnisliste einen Unternehmensbereich. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 8: Eigenschaften von Unternehmensbereichen

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

Eigenschaft	Beschreibung
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in diesem Unternehmensbereich zulässig sind. Dieser Wert kann bei der Regelprüfung ausgewertet werden. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn dasModul 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 Geschäftsrollen Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows für die Attestierungsvorgänge als verantwortliche Attestierer herangezogen werden. Dazu ordnen Sie den Geschäftsrollen 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 9: Standardanwendungsrolle für Attestierer

Benutzer	Aufgaben
Attestierer für Geschäftsrollen	Die Attestierer müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Attestierer** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Geschäftsrollen, für die sie verantwortlich sind. • Können die Stammdaten der Geschäftsrollen sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Um Attestierer festzulegen

1. Wählen Sie die Kategorie **Geschäftsrollen | Basisdaten zur Konfiguration | Attestierer**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Person und doppelklicken Sie .
4. Speichern Sie die Änderungen.

Genehmiger und Genehmiger (IT)

Im One Identity Manager können Sie an Geschäftsrollen Personen zuweisen, die bei entsprechender Einrichtung der Entscheidungsworkflows als verantwortliche Entscheider für Genehmigungsverfahren bei IT Shop-Bestellungen herangezogen werden. Dazu ordnen Sie den Geschäftsrollen die 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 10: Standardanwendungsrollen für Genehmiger

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

Um Genehmiger oder Genehmiger (IT) festzulegen

1. Wählen Sie die Kategorie **Geschäftsrollen| Basisdaten zur Konfiguration | Genehmiger**.

   - ODER -

   Wählen Sie die Kategorie **Geschäftsrollen | 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.

Geschäftsrollen bearbeiten

Geschäftsrollen werden in der Navigationsansicht nach Rollenklassen gruppiert. Jede Geschäftsrolle ist genau einer Rollenklasse zugeordnet. Bevor Sie Geschäftsrollen anlegen können, definieren Sie dafür geeignete Rollenklassen. Weitere Informationen finden Sie unter Rollenklassen auf Seite 27.

Um Geschäftsrollen zu bearbeiten

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Allgemeine Stammdaten einer Geschäftsrolle

Für eine Geschäftsrolle erfassen Sie die folgenden allgemeine Stammdaten.

Tabelle 11: Allgemeine Stammdaten einer Geschäftsrolle

Eigenschaft	Beschreibung
Geschäftsrolle	Bezeichnung der Geschäftsrolle.

Eigenschaft	Beschreibung
Kurzname	Kurzbezeichnung der Geschäftsrolle
Interner Name	Zusätzliche Bezeichnung der Geschäftsrolle.
Rollenklasse	Rollenklasse, der die Geschäftsrolle zugeordnet ist. Der Wert ist durch die in der Navigationsansicht ausgewählte Rollenklasse vorbelegt. Wenn Sie eine Geschäftsrolle neu anlegen, können Sie eine beliebige Rollenklasse zuweisen.
Übergeordnete Geschäftsrolle	Übergeordnete Geschäftsrolle in der Rollenhierarchie. Um Geschäftsrollen hierarchisch zu organisieren, wählen Sie in der Auswahlliste die übergeordnete Geschäftsrolle aus. Es stehen dabei nur die Geschäftsrollen zur Auswahl, die zur selben Rollenklasse gehören. Für eine Geschäftsrolle, die in der obersten Ebene einer Geschäftsrollenhierarchie steht, lassen Sie dieses Eingabefeld leer.
Rollentyp	Wählen Sie einen Rollentyp aus der Auswahlliste aus. Um einen neuen Rollentyp zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung und eine Beschreibung des Rollentyps.
Genehmiger	Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieser Geschäftsrolle 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 Geschäftsrolle entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Manager	Verantwortlicher Manager der Geschäftsrolle.
2. Verantwortlicher	Stellvertretender Manager der Geschäftsrolle.
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge für die Geschäftsrolle 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 Geschäftsrolle primär zugeordnet ist.

Eigenschaft	Beschreibung
Standort	Standort, dem die Geschäftsrolle primär zugeordnet ist.
Kostenstelle	Kostenstelle, der die Geschäftsrolle primär zugeordnet ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Zertifizierungsstatus	Zertifizierungsstatus der Geschäftsrolle. Folgende Zertifizierungsstatus können ausgewählt werden. • Neu – Die Geschäftsrolle wurde neu in der One Identity Manager-Datenbank angelegt. • Zertifiziert – Die Stammdaten der Geschäftsrolle wurden durch einen Manager genehmigt. • Abgelehnt – Die Stammdaten der Geschäftsrolle wurden durch einen Manager nicht genehmigt.
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Vererbung blockieren	Angabe, ob die Vererbung an diese Geschäftsrolle unterbrochen wird. Aktivieren Sie diese Option, um die Vererbung innerhalb der Geschäftsrollenhierarchie zu unterbrechen.
X500 Knoten	Aktivieren Sie diese Option, um die Geschäftsrolle für den Export in ein X500-Schema zu kennzeichnen.
Keine Vererbung an Personen	Angabe, ob die Vererbung an Personen für diese Geschäftsrolle vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Angabe, ob die Vererbung an Geräte für diese Geschäftsrolle vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Angabe, ob die Vererbung an Arbeitsplätze für diese Geschäftsrolle vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Angabe, ob für die Geschäftsrolle eine dynamische Rolle erstellt werden darf.

Verwandte Themen

- Rollenklassen auf Seite 27
- Rollentypen auf Seite 28
- Genehmiger und Genehmiger (IT) auf Seite 31
- Attestierer auf Seite 30
- Einschränken der Vererbung über Geschäftsrollen auf Seite 22
- Dynamische Rolle erstellen auf Seite 46

Adressinformationen einer Geschäftsrolle

Erfassen Sie die folgenden Stammdaten zur Erreichbarkeit der Geschäftsrolle.

Tabelle 12: Adressdaten einer Geschäftsrolle

Eigenschaft	Beschreibung
Adresse	Postanschrift der Geschäftsrolle.
Straße	Straße.
Gebäude	Gebäude.
Postleitzahl	Postleitzahl.
Ort	Ort.
Land	Land. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln. Weitere Informationen finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.
Bundesland	Bundesland. Die Angabe wird benötigt, um die Sprache und die Arbeitszeiten einer Person zu ermitteln. Weitere Informationen finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.
Telefon	Telefonnummer der Geschäftsrolle.
Telefonkurzangabe	Telefonkurzwahl (ohne Vorwahl).
Raum	Raum.
Bemerkung (Raum)	Freitextfeld für zusätzliche Erläuterungen.

Unternehmensbereich und Risikobewertung

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

Tabelle 13: Stammdaten zum Unternehmensbereich einer Geschäftsrolle

Eigenschaft	Beschreibung
Unternehmensbereich	Unternehmensbereich der Abteilung. Die Angabe wird zur Risikobewertung der Abteilung benötigt. Weitere Informationen finden Sie unter Unternehmensbereiche auf Seite 28.

Eigenschaft	Beschreibung
Risikoindex (berechnet)	Für die Risikobewertung der Abteilung wird anhand der zugewiesenen Unternehmensressourcen ein Risikoindex berechnet. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist. Ausführliche Informationen dazu finden Sie im One Identity Manager Administrationshandbuch für Risikobewertungen.
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen an die Abteilung sind. Stellen Sie über den Schieberegler einen Wert zwischen 0 und 1 ein. 0 ... keine Transparenz 1 ... volle Transparenz
Max. Anzahl Regelverletzungen	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 Geschäftsrolle.
Gewinn des Bereichs	Gewinn der Geschäftsrolle.

Benutzerdefinierte Stammdaten einer Geschäftsrolle

Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Personen, Geräte und Arbeitsplätze an Geschäftsrollen zuweisen

Damit Unternehmensressourcen an Personen, Geräte und Arbeitsplätze vererbt werden können, müssen Sie diese Objekte an Rollen zuweisen.

Um Personen, Geräte und Arbeitsplätze in eine Geschäftsrolle aufzunehmen

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.

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 Geschäftsrollen zuzuweisen.

Verwandte Themen

- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 21
- Unternehmensressourcen an Geschäftsrollen zuweisen auf Seite 37
- Dynamische Rolle erstellen auf Seite 46

Unternehmensressourcen an Geschäftsrollen 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 Geschäftsrollen 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 Geschäftsrolle 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 Geschäftsrollen 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 14: Mögliche Zuweisungen von Unternehmensressourcen an Rollen

Unternehmensressource	Verfügbar im Modul
Ressourcen	immer
Kontendefinitionen	Zielsystem Basismodul
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
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
Applikationen	Modul Applikationsmanagement

Unternehmensressource	Verfügbar im Modul
Azure Active Directory Gruppen	Azure Active Directory Modul
Azure Active Directory Administratorrollen	Azure Active Directory Modul
Azure Active Directory Abonnements	Azure Active Directory Modul
Unwirksame Azure Active Directory Dienst-pläne	Azure Active Directory Modul
Unix Gruppen	Modul Unix-basierte Zielsysteme
Cloud Gruppen	Modul Cloud Systems Management
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 **Geschäftsrollen | <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 10
- Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 21

Verwandte Themen

- Mögliche Zuweisungen von Unternehmensressourcen auf Seite 18
- Personen, Geräte und Arbeitsplätze an Geschäftsrollen zuweisen auf Seite 36
- Dynamische Rolle erstellen auf Seite 46

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, 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 15: 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.

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, Standorten und Geschäftsrollen definiert. Einer Person wird eine primäre Abteilung, eine primäre Kostenstelle, ein primärer Standort oder eine primäre Geschäftsrolle zugeordnet. Abhängig von dieser Zuordnung werden die gültigen IT Betriebsdaten ermittelt und für die Erstellung des Benutzerkontos verwendet. Können über die primären Rollen keine gültigen IT Betriebsdaten ermittelt werden, werden die Standardwerte verwendet.

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

Beispiel

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

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

Für die Abteilung A legen Sie die wirksamen IT Betriebsdaten für die Domäne A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet.

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste eine Rolle.
3. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten** und erfassen Sie folgende Daten.

Tabelle 16: IT Betriebsdaten

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

4. 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 17: 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

Zielsystemtyp	IT Betriebsdaten
SharePoint Online	Gruppen erbbar
	Privilegiertes Benutzerkonto
	Authentifizierungsmodus
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

Zielsystemtyp	IT Betriebsdaten
G Suite	Organisation
	Identität
	Gruppen erbbar
	Privilegiertes Benutzerkonto
	Kennwort bei der nächsten Anmeldung ändern

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 Geschäftsrolle 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 Geschäftsrolle, 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, den die Objekteigenschaft durch die Änderung an den

Wert: IT Betriebsdaten annehmen würde.

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zusätzliche Aufgaben zur Verwaltung von Geschäftsrollen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können. Die wichtigsten Informationen erhalten Sie über das Überblicksformular.

Dynamische Rolle erstellen

Über diese Aufgabe definieren Sie dynamische Rollen für einzelne Geschäftsrollen. 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 Geschäftsrolle zugewiesen werden; verlässt eine Person diese Geschäftsrolle verliert sie sofort die zugewiesenen Unternehmensressourcen.

Rollenmitgliedschaften über dynamische Rollen werden als 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. Weitere Informationen finden Sie unter Zuweisung von Personen, Geräten, Arbeitsplätzen und Unternehmensressourcen erlauben auf Seite 21.

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

Um eine dynamische Rolle zu erstellen

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>.**
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle.
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 **Geschäftsrollen | <Rollenklasse> | Dynamische Rollen**.
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle.
3. Öffnen Sie das Überblicksformular der Geschäftsrolle.
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.

Ausführliche Informationen zum Erstellen und Bearbeiten dynamischer Rollen finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

Verwandte Themen

- Allgemeine Stammdaten einer Geschäftsrolle auf Seite 32

Organisationen zuweisen

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

Um eine Abteilung, eine Kostenstelle oder einen Standort an Geschäftsrollen zuzuweisen

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**, **Organisationen | Kostenstellen** oder **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

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

   Die ausgewählte Rolle wird allen Geschäftsrollen als Abteilung, Kostenstelle beziehungsweise Standort primär zugewiesen.

   - ODER -

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

Vererbungsausschluss für Geschäftsrollen 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 Geschäftsrollen 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 Geschäftsrollen festzulegen

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle.
3. Wählen Sie die Aufgabe **Widersprechende Geschäftsrollen bearbeiten**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu, die sich mit der gewählten Geschäftsrolle ausschließen.

   - ODER -

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

Detaillierte Informationen zum Thema

- Vererbungsausschluss: Festlegen widersprechender Rollen auf Seite 24

Zusatzeigenschaften zuweisen

An Geschäftsrollen können Sie Zusatzeigenschaften zuweisen. Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche. Weitere Informationen finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

Um Zusatzeigenschaften für eine Geschäftsrolle festzulegen

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
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.

Zuweisungsressource erzeugen

Es ist möglich, Zuweisungsressourcen für einzelne Geschäftsrollen anzulegen. Damit können Zuweisungsbestellungen im Web Portal auf einzelne Geschäftsrollen eingeschränkt werden. Bei der Bestellung der Zuweisungsressource ist es nicht mehr notwendig, die Geschäftsrolle zusätzlich auszuwählen. Sie ist automatisch Bestandteil der Zuweisungsbestellung. Weitere Informationen finden Sie im Handbuch One Identity Manager Administrationshandbuch für IT Shop.

Um eine Zuweisungsressource auf eine Geschäftsrolle einzuschränken

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>.**
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle.
3. Wählen Sie die Aufgabe **Zuweisungsressource erzeugen...**.

   Es wird ein Assistent gestartet, der Sie durch das Anlegen der Zuweisungsressource führt.

Berichte über Geschäftsrollen

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 Geschäftsrollen stehen folgende Berichte zur Verfügung.

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

Tabelle 18: Berichte über Geschäftsrollen

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Rollen, in denen die Personen der ausgewählten Geschäftsrolle ebenfalls Mitglied sind.
Historische Mitgliedschaften anzeigen	Der Bericht listet alle Mitglieder der ausgewählten Geschäftsrolle und den Zeitraum ihrer Mitgliedschaft auf.
Zu entscheidende Produkte anzeigen	Der Bericht zeigt für eine Geschäftsrolle alle Produkte, deren Bestellungen durch Mitglieder der Geschäftsrolle genehmigt werden können.
Geschäftsrollen mit hohem Risikoindex	Der Bericht listet alle Geschäftsrollen mit einem Risikoindex gleich oder höher als den konfigurierbaren Risikoindex. Das Ergebnis kann auf eine bestimmte Rollenklasse eingeschränkt werden. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.

Verwandte Themen

- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 40

2

Role Mining im One Identity Manager

Die Gestaltung von Geschäftsrollen kann auf zwei Wegen erfolgen:

- Rollenmodellierung wie unter Geschäftsrollen verwalten auf Seite 5 beschrieben.
- Analyse der existierenden Berechtigungen, das sogenannte Role Mining.

Mit dem Programm "Analyzer" stellt der One Identity Manager eigenes Werkzeug für die Analyse der Benutzerkonten und Berechtigungen zur Verfügung. Der Analyzer unterstützt die von Geschäftsrollen genauso wie die Analyse der Datenqualität in Bezug auf die Frage: Wie gut sind die Berechtigungsdaten für eine teilautomatisierte Rollenbildung geeignet?

Der Analyzer bietet:

- die automatische Analyse von Berechtigungszuordnungen auf Basis von Clusteranalyse Algorithmen mit unterschiedlichen Wichtungen
- die automatische Analyse existierender Strukturen und der Berechtigungen der dort zugeordneten Personen
- eine manuelle Analyse bestimmter Mitarbeitergruppen zur Rollenbildung

Ziel der Rollenbildung ist es, direkte Berechtigungen, die bisher in einzelnen Anwendungssystemen für Benutzer vergeben wurden, durch indirekte zu ersetzen. Dabei können Berechtigungen, die Benutzer über die Zugehörigkeit in einer Rolle erhalten, auch Anwendungssystem übergreifend definiert werden. Das Ziel des Analyzers ist dabei nicht nur die reine Rollenbildung, sondern auch die Einordnung der Rollen in ein einfach zu administrierendes Hierarchiesystem. So kann der Verwaltungsaufwand weiter reduziert und die Sicherheit bei der Berechtigungsvergabe erhöht werden.

Um das Role Mining im One Identity Manager zu nutzen

- Aktivieren Sie im Designer den Konfigurationsparameter "QER\Org\RoleMining".

HINWEIS: Um den Analyzer für die Analyse von Berechtigungen zu nutzen, muss mindestens das Zielsystem Basismodul vorhanden sein.

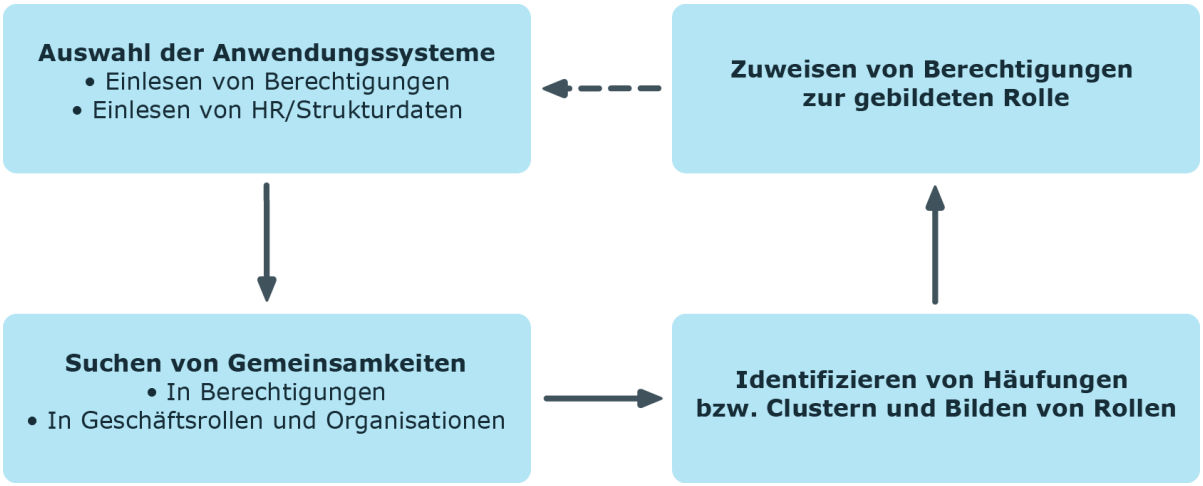
Clusteranalyse als Grundlage des Role Mining

Grundlage des Role Mining ist immer eine Clusteranalyse, bei Analyzer mit Hilfe eines mathematischen Algorithmus versucht, einzelne Cluster, also Personen mit ähnlichen Berechtigungen, zu finden. Dabei werden entweder hierarchische Strukturen gebildet oder vorgegebene Strukturen genutzt, die für den Aufbau eines eigenen Rollenmodells genutzt werden können.

Beim Role Mining versucht man allerdings nicht nur, einzelne Cluster zu finden und diese dann Geschäftsrollen zuzuweisen. Vielmehr ist es sinnvoll, direkt hierarchische Rollenstrukturen zu entwickeln, die dann über die gängigen Vererbungsmechanismen effizient nutzbar sind.

Automatisiertes Role Mining unterstützt der One Identity Manager durch zwei verschiedene Clusteranalyseverfahren, die sich durch die Berechnung der Abstände zwischen einzelnen Clustern unterscheiden. Auch die Verwendung von bereits vorhandenen Rollenstrukturen, beispielsweise organisatorische Strukturen aus ERP-Systemen, ist möglich. Mit Hilfe der Berechtigungsanalyse können diesen dann Rechte zugewiesen werden. Zuletzt können Rollenstrukturen frei definiert und die Zuordnung von Berechtigungen und Personen an Hand der vorhandenen Berechtigungen manuell bewertet werden.

Abbildung 14: Clusteranalyse-Verfahren im Analyzer



Bei den Clusteringverfahren berechnet der Analyzer aus Berechtigungen eines Benutzers in den verschiedenen Anwendungssystemen, wie Active Directory, IBM Notes oder SAP R/3, eine Häufigkeitsverteilung. Dabei kann einzelnen Berechtigungen im Vergleich zu anderen eine höhere Wichtigkeit eingeräumt werden. So kann beispielsweise die Anzahl der Mitglieder einer Berechtigung ein solches Kriterium darstellen. Dies wird durch den Analyzer bei der Berechnung erkannt und durch Gewichtung bei der Abstandsbetrachtung zwischen den einzelnen Clustern berücksichtigt. So können die bei der Analyse entstehenden hierarchische Strukturen bereits im Vorfeld optimiert und eine möglichst kleine Anzahl von Rollen erzielt werden.

Arbeiten mit dem Programm Analyzer

Mit dem Analyzer können Sie Datenkorrelationen in der Datenbank automatisch analysieren und erkennen. Diese Informationen können genutzt werden, um zum Beispiel direkte Berechtigungszuordnungen durch indirekte Zuordnungen zu ersetzen, und somit den Verwaltungsaufwand zu reduzieren.

Menüeinträge

Tabelle 19: Bedeutung der Einträge in der Menüleiste

Menü	Menüeintrag	Bedeutung	Tastenkombination
Datenbank	Neue Verbindung...	Es wird eine Datenbankverbindung hergestellt.	Strg + Shift + N
	Übertragung in Datenbank...	Die geänderten Zuordnungen werden in die verbundene One Identity Manager-Datenbank übertragen.	Strg + Shift + S
	Einstellungen...	Es können allgemeine Programmeinstellungen konfiguriert werden.	
	Beenden	Das Programm wird beendet.	Alt + F4
Analyse	Vorherige Zuweisung	Es wird zur vorherigen Zuweisung der Person/Berechtigung gesprungen.	Strg + U
	Nächste Zuweisung	Es wird zur nächsten Zuweisung der Person/Berechtigung gesprungen.	Strg + D
	Übergeordneter Knoten	Es wird zum übergeordneten Knoten im Strukturbaum gewechselt.	Strg + P
	Neu analysieren	Die Analyse wird erneut ausgeführt.	F9
Hilfe	Hilfe zum Analyzer	Die Hilfe zum angezeigten Programm wird geöffnet.	F1
	Info...	Die Versionsinformationen zum Programm werden angezeigt.	

Anpassen der Programmeinstellungen

Um Programmeinstellungen zu ändern

- Wählen Sie den Menüeintrag **Datenbank | Einstellungen...**.

Tabelle 20: Programmeinstellungen

Einstellung	Bedeutung
Informationsfenster zur Datenanalyse am Ende automatisch schließen	Ist die Option aktiviert, wird bei vordefinierten Analysen das Informationsfenster am Ende der Analyse geschlossen. Ist die Option nicht aktiviert, wird das Informationsfenster angezeigt. Dieses Fenster beenden Sie über die Schaltfläche **Fertig**.
Wichtung der Berechtigungen anzeigen	Aktivieren Sie diese Option, um zusätzlich eine Wichtung der Berechtigungen anzuzeigen.
Bildungsregel für den Rollennamen	Legen Sie die Bildungsregel für Rollennamen fest. Diese wird bei der Bildung neuer Rollennamen bei vordefinierten Analyseverfahren angewendet. Die Bildungsregel unterstützt folgende Variablen: %sequence% Fortlaufende Nummer %object% Name des ersten Objekts im Cluster %property% Name der ersten Eigenschaft im Cluster

Durchführen einer Analyse

Um eine Analyse mit dem Analyzer zu starten

- Wählen Sie **Start | One Identity | One Identity Manager | Analyzer**.
- Geben Sie die Verbindungsdaten zur Datenbank und die Systembenutzerkennung ein und melden Sie sich am Programm an.
- Wählen Sie ein Analyseverfahren aus.

Tabelle 21: Analysemethode

Analysemethode	Beschreibung
Analysedaten mit	Die Ausgangsdaten werden mit einem Assistenten

Analysemethode	Beschreibung
dem Assistenten wählen	zusammengestellt. Weitere Informationen finden Sie unter Analysedaten mit dem Assistenten auswählen auf Seite 55.
Active Directory Berechtigungen der Personen	Es werden die Berechtigungen alle Personen mit Active Directory Gruppenmitgliedschaften analysiert. Weitere Informationen finden Sie unter Vordefinierte Analysen auf Seite 58. HINWEIS: Die Analysemethode steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.
Active Directory Berechtigungen und Abteilungen der Personen	Es werden die Berechtigungen alle Personen mit Active Directory Gruppenmitgliedschaften analysiert. Zusätzliche werden Abteilungen mit Active Directory Gruppen in die Analyse einbezogen. Weitere Informationen finden Sie unter Vordefinierte Analysen auf Seite 58. HINWEIS: Die Analysemethode steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

- Prüfen Sie die Analyseergebnisse. Weitere Informationen finden Sie unter Auswertung der Analyse auf Seite 58.
- Erstellen Sie bei Bedarf neue Geschäftsrollen und ordnen Sie die Personen zu. Übernehmen Sie die vorgeschlagenen Änderungen in die One Identity Manager-Datenbank. Weitere Informationen finden Sie unter Übernahme der Änderungen auf Seite 61.

Analysedaten mit dem Assistenten auswählen

Zu Beginn der Analyse stellen Sie die Ausgangsdaten zusammen. Der Analyzer greift auf sämtliche in seiner eigenen Datenbank vorhandenen Berechtigungsinformationen zurück und erstellt eine Zuordnungstabelle mit Personen und ihren Berechtigungen. Ergebnis können Vorschläge für Einzelrollen aus der Analyse eines einzelnen Anwendungssystems oder auch systemübergreifende Rollen aus der Analyse von Berechtigungen mehrerer Systeme sein.

Um die Ausgangsdaten auszuwählen

1. Wählen Sie auf der Startseite des Analyzers den Eintrag **Analysedaten mit Assistenten wählen.**
2. Klicken Sie die Schaltfläche **Start**.
3. Legen Sie den Personenkreis zur Analyse fest. Wählen Sie eines der folgenden Auswahlverfahren.

- Strukturen

  Die Auswahl der Personen erfolgt über die im One Identity Manager enthalten Organisationen und Geschäftsrollen.

  a. Wählen Sie das Auswahlverfahren **Strukturen**.

  b. Klicken Sie **Weiter**.

  c. Wählen Sie in der Liste **Strukturen** die Organisation oder Geschäftsrolle zur Analyse aus.

  In der Liste **Personen** werden die Personen angezeigt, die der Struktur zugeordnet sind. Über die Symbole im rechten Bereich der Personenliste können Sie die angezeigten Personen weiter filtern.

  Tabelle 22: Symbole zum Filtern der Personenliste

Symbol	Bedeutung
	Indirekt zugeordnete Personen anzeigen.
	Direkt zugeordnete Personen anzeigen.
	Personen untergeordneter Strukturen anzeigen.

  d. Klicken Sie **Weiter**.

- Filterassistent

  Legen Sie die Bedingung fest, anhand der die Personen aus der Datenbank ermittelt werden. Der Assistent unterstützt Sie bei der Formulierung einer Bedingung (Where-Klausel) für Datenbankabfragen. Die komplette Datenbankabfrage wird intern zusammengesetzt. Die Datenbankabfrage bezieht sich auf die Tabelle „Person". Weitere Informationen zum Umgang mit dem Assistenten finden Sie im One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge.

- Auswahlliste

  In der Liste werden alle Personen der One Identity Manager-Datenbank angezeigt. Über **Shift + Auswahl** oder **Strg + Auswahl** wählen Sie mehrere Personen zur Analyse aus.

- Assistentenvorlage laden

  Laden Sie eine vorhandene Konfiguration. Wählen Sie die Vorlagedatei und klicken Sie **Öffnen**.

4. Klicken Sie **Weiter**.
5. Wählen Sie das Zielsystem, dessen Benutzerkonten und Berechtigungen in die Analyse einbezogen werden. Über **Strg + Auswahl** können Sie mehrere Zielsystem auswählen.
6. Klicken Sie **Weiter**.

7. Legen Sie das Analyseverfahren fest. Zur Auswahl stehen folgende Verfahren.

Tabelle 23: Analyseverfahren

Analyseverfahren	Beschreibung
Einfache Clusteranalyse/Komplexe Clusteranalyse	Die Berechtigungen werden mittels Clusteranalyseverfahren zu neuen Geschäftsrollen gruppiert und die Personen zugeordnet. Der Analyzer unterstützt das automatisierte Role Mining durch zwei verschiedene Clusteranalyseverfahren, die sich durch die Berechnung der Abstände zwischen einzelnen Clustern unterscheiden
Entscheidungsbaum	Die Berechtigungen werden in einem Entscheidungsbaum zu neuen Geschäftsrollen gruppiert und die Personen zugeordnet. Als Entscheidungsmerkmal wird die Anzahl der Gruppenmitglieder genutzt.
Strukturzuordnung	Die Berechtigungen werden einem bestehendem Strukturbaum zugeordnet. Die Verwendung von bereits vorhandenen Strukturen, beispielsweise organisatorische Strukturen aus ERP-Systemen, ist möglich.
Berechtigungsanalyse	Mit Hilfe der Berechtigungsanalyse werden die Berechtigungen der Personen analysiert. Geschäftsrollen werden frei definiert und die Zuordnung von Berechtigungen und Personen an Hand der vorhandenen Berechtigungen manuell bewertet.

8. Klicken Sie **Weiter**.
9. (Optional) Um die Konfiguration zu einem späteren Zeitpunkt wieder zu verwenden, aktivieren Sie die Option **Konfiguration als Vorlagedatei speichern**. Wählen Sie über den Dateibrowser den Ablagepfad, geben Sie einen Dateinamen und klicken Sie **Speichern**.
10. Klicken Sie **Fertig**, um die Analyse zu starten.

    Die Analyseinformationen werden geladen und die Analyse gestartet. Anschließend werden die Analyseergebnisse dargestellt. Weitere Informationen finden Sie unter Auswertung der Analyse auf Seite 58.
11. Erstellen Sie bei Bedarf neue Geschäftsrollen und ordnen Sie die Personen zu. Übernehmen Sie die vorgeschlagenen Änderungen in die One Identity Manager-Datenbank. Weitere Informationen finden Sie unter Übernahme der Änderungen auf Seite 61.

Vordefinierte Analysen

HINWEIS: Die Analysemethoden stehen zur Verfügung, wenn das Active Directory Modul vorhanden ist.

Es werden folgende vordefinierte Analysen zur Verfügung gestellt:

- Active Directory Berechtigungen der Personen

  Es werden die Berechtigungen alle Personen mit Active Directory Gruppenmitgliedschaften analysiert.

- Active Directory Berechtigungen und Abteilungen der Personen

  Es werden die Berechtigungen alle Personen mit Active Directory Gruppenmitgliedschaften analysiert. Zusätzliche werden Abteilungen mit Active Directory Gruppen in die Analyse einbezogen.

Um eine vordefinierte Analyse zu starten

1. Wählen Sie auf der Startseite des Analyzers den Eintrag **Active Directory Berechtigungen der Personen** oder den Eintrag **Active Directory Berechtigungen und Abteilungen der Personen**.
2. Klicken Sie **Start**.

   Die Analyseinformationen werden geladen und die Analyse wird sofort gestartet. Abhängig von der Datenmenge, kann die Analyse einige Zeit in Anspruch nehmen.

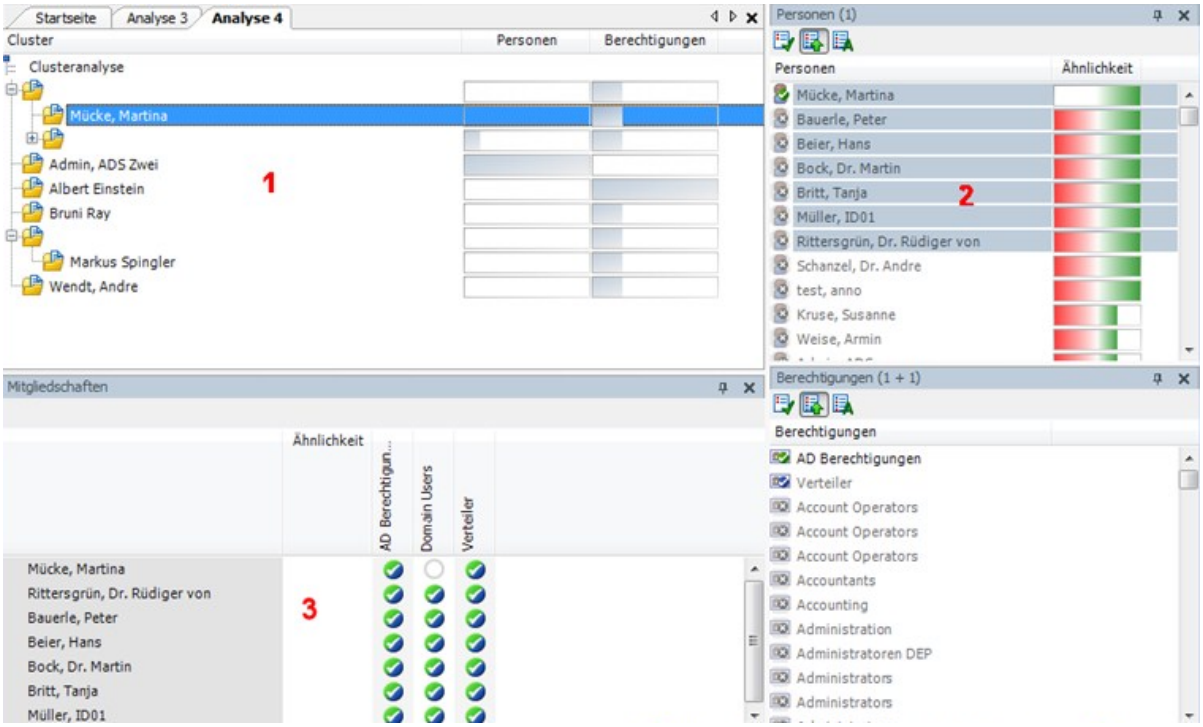
   Abhängig von den Programmeinstellungen werden Informationen zur Analyse angezeigt. Über **Erweitern...** sehen Sie detaillierte Informationen. Über **Fertig** schließen Sie das Informationsfenster. Anschließend werden die Analyseergebnisse dargestellt. Weitere Informationen finden Sie unter Auswertung der Analyse auf Seite 58.

Auswertung der Analyse

Da das mathematische Verfahren der Clusteranalyse nur einen Trend vorgibt, sollten Sie beim Role Mining die Geschäftsrollen immer mit den unternehmensspezifischen Strukturen abgleichen. Neben der Umbenennung von Knoten können Sie Zuweisungen der Personen und Berechtigungen einer Geschäftsrolle auch direkt bearbeiten. Mit dem Analyzer können Sie neue Geschäftsrollen erstellen und Personen direkt zuordnen. Das Hinzufügen oder das Verschieben von Personen in eine bestimmte Geschäftsrolle lässt sich damit einfach umsetzen.

Der Analyzer zeigt das Ergebnis seiner Analyse in einem mehr geteilten Bildschirm an.

Abbildung 15: Darstellung der Analyseergebnisse



Im oberen linken Bereich (1) werden die durch die Analyse gefundenen Cluster in einem Strukturbaum angezeigt. Die Benennung der gebildeten Knoten erfolgt bei der Auswahl der Analysedaten mittels Assistenten durch die zuerst gefundene Person. Bei vordefinierten Analyseverfahren richtet sich die Benennung nach der in den Programmeinstellungen festgelegten Regel. Die Bezeichnungen der können Sie über **F2** oder das Kontextmenü **Umbenennen** ändern.

In den Spalten Personen und Berechtigungen grafisch die Anzahl der Vorkommen abgebildet. Bei beiden Spalten wird die Anzeige normiert, das heißt die Gruppe mit der höchsten Anzahl von zugeordneten Personen oder Berechtigungen entspricht 100% und wird mit maximalen Balken dargestellt.

Tabelle 24: Bedeutung der Einträge im Kontextmenü im Bereich 1

Eintrag im Kontext-menü	Bedeutung
Einfügen	Die Geschäftsrolle wird zur Übernahme in die Datenbank gekennzeichnet.
Rekursiv einfügen	Die Geschäftsrolle und ihre untergeordneten Geschäftsrollen werden zur Übernahme in die Datenbank gekennzeichnet.
Löschen	Die Geschäftsrolle wird aus der Datenübernahme entfernt.
Anlegen	Es wird eine neue Geschäftsrolle definiert.
Löschen	Die Geschäftsrolle wird gelöscht.

Eintrag im Kontext-menü	Bedeutung
Umbenennen	Die Geschäftsrolle wird umbenannt.
Geschäftsrollennamen generieren	Die Bezeichnungen der Geschäftsrollen werden entsprechend der festgelegten Regel (Menü <Datenbank>\<Einstellungen...>) erzeugt.
Geschäftsrollen optimieren	Die Geschäftsrollen werden optimiert. Leere Geschäftsrollen werden gelöscht.
Eigenschaften	Es werden weitere Eigenschaften der Geschäftsrolle wie Benutzerkonten und Berechtigungen angezeigt.

Bei der Auswahl eines Strukturknotens werden im rechten Bereich (2), die in ihm enthaltenen Personen (oben) und Berechtigungen (unten) aufgelistet. Für Personen können Sie mit Hilfe einer farbigen Ähnlichkeitsdarstellung feststellen, bei welchen Berechtigungen es untereinander Übereinstimmungen gibt und in wie weit die tatsächliche Berechtigungssituation des Benutzers zu der Berechtigungszuordnung der gewählten Rolle passt. Übereinstimmende Gruppenmitgliedschaften werden grün, während abweichende, zusätzliche Gruppenmitgliedschaften rot angezeigt werden. Direkt darunter werden die einzelnen Berechtigungen von Personen in den analysierten Zielsystemen angezeigt. Abhängig von den Programmeinstellungen wird zusätzlich eine Wichtung der Berechtigungen angezeigt.

Tabelle 25: Bedeutung der Einträge im Kontextmenü im Bereich (2)

Eintrag im Kontextmenü	Bedeutung
Zur Geschäftsrolle hinzufügen	Die Person/Berechtigung wird zur im Strukturbaum ausgewählten Geschäftsrolle hinzugefügt.
Aus Geschäftsrolle entfernen	Die Person/Berechtigung wird aus der im Strukturbaum ausgewählten Geschäftsrolle entfernt.
Vergleichen	Die Personen werden miteinander verglichen. Die Anzeige erfolgt im Bereich 3.
Zuweisungen markieren	Die Zuweisungen der Person/Berechtigung werden im Strukturbaum markiert.
Eigenschaften	Es werden weitere Eigenschaften des aktiven Objekts angezeigt.

Durch eine Mehrfachauswahl in der Personenliste können Sie die Berechtigungsmitgliedschaften einzelner Personen im linken unteren Bereich (3) weiter analysieren und direkt mit anderen Personen vergleichen.

Um Mitgliedschaften von Personen zu vergleichen

- Wählen Sie im rechten Bereich (2) die Personen mittels aus **Strg + Auswahl** oder **Shift + Auswahl** aus.
- Starten Sie über den Kontextmenüeintrag **Vergleichen** den Vergleich.

TIPP: Durch die Auswahl einer Person in diesem Bereich per Mausklick legen Sie diese Person als Referenzperson in der Anzeige fest. Die farbliche Ähnlichkeitskennung wird an dieser Person ausgerichtet.

Übernahme der Änderungen

Mit dem Analyzer können Sie neue Geschäftsrollen erstellen und Personen direkt zuordnen oder Personen und Berechtigungen in bestimmte Geschäftsrollen verschieben.

Um die Änderungen in die One Identity Manager-Datenbank zu übertragen

1. Markieren Sie im Strukturbaum die Geschäftsrollen, die Sie übernehmen möchten.

   Verwenden Sie dazu die Kontextmenüeinträge **Einfügen** bzw. **Rekursiv einfügen**. Einzelne Geschäftsrollen können Sie über den Kontextmenüeintrag **Entfernen** aus der Datenübernahme löschen.
2. Starten Sie über den Menüeintrag **Datenbank | Übertragung in die Datenbank...** den Assistenten zur Datenübernahme und klicken Sie im Assistenten **Weiter**.
3. Wählen Sie im Assistenten die Rollenklasse unterhalb der die Geschäftsrollen in der One Identity Manager-Datenbank erzeugt werden.

   Über die Schaltfläche neben der Auswahlliste können die eine neue Rollenklasse erstellen.

4. Wählen Sie die Speicheroptionen.

Tabelle 26: Speicheroptionen für die Datenübernahme

Speicheroption	Bedeutung
Vorhandene Objekte in der Rollenklasse löschen	Bereits in der One Identity Manager-Datenbank vorhandene Objekte in der gewählten Rollenklasse werden gelöscht.
Vererbung an Geschäftsrollen deaktivieren	Die Vererbung von Zuweisungen an Geschäftsrollen ist deaktiviert. HINWEIS: Nachdem Sie die Zuordnungen geprüft haben, entfernen Sie die Option **Keine Vererbung an Personen** an den Geschäftsrollen. Verwenden Sie dazu das Programm "Manager".
Direkte Zuordnungen entfernen	Direkte Zuordnungen von Berechtigungen zu den Benutzerkonten der Personen werden entfernt. **VORSICHT: Setzen Sie diese Option nur, wenn Sie sicher gestellt haben, dass die Berechtigungen über Geschäftsrollen an die Personen vererbt werden. Anderenfalls führt diese Option zum Verlust der Berechtigungen.**
Neu angelegte Rollen attestieren	Die neuen Geschäftsrollen müssen einen Attestierungsvorgang durchlaufen. HINWEIS: Diese Funktion steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

5. Klicken Sie **Fertig**, um die Daten zu übernehmen.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

U

V

W

Z