



One Identity Manager 9.3

Administrationshandbuch für
Geschäftsrollen

Copyright 2025 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

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

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

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

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

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



Patente

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

Marken

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

Legende

-  **WARNUNG:** Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.
-  **VORSICHT:** Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

One Identity Manager Administrationshandbuch für Geschäftsrollen
Aktualisiert - 06. Januar 2025, 12:22 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter [Dokumentation](#).

Inhalt

Geschäftsrollen verwalten	6
One Identity Manager Benutzer für Geschäftsrollen	7
Grundlagen für den Aufbau von hierarchischen Rollen	8
Vererbungsrichtungen innerhalb einer Hierarchie	9
Unterbrechen der Vererbung	11
Grundlagen zur Zuweisung von Unternehmensressourcen	13
Direkte Zuweisung von Unternehmensressourcen	14
Indirekte Zuweisung von Unternehmensressourcen	14
Sekundäre Zuweisung von Unternehmensressourcen	14
Primäre Zuweisung von Unternehmensressourcen	15
Zuweisung von Unternehmensressourcen über dynamische Rollen	16
Zuweisung von Unternehmensressourcen über IT Shop Bestellungen	17
Grundlagen zur Berechnung der Vererbung	17
Berechnung der Vererbung über hierarchische Rollen	18
Berechnung der Zuweisungen	20
Vorbereiten der Geschäftsrollen für die Zuweisung von Unternehmensressourcen	22
Mögliche Zuweisungen von Unternehmensressourcen über Geschäftsrollen	22
Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben	27
Festlegen der Vererbungsrichtung	28
Vererbung über Geschäftsrollen blockieren	29
Vererbung an Identitäten, Geräte oder Arbeitsplätze für einzelne Geschäftsrollen verhindern	29
Vererbung an einzelne Identitäten, Geräte oder Arbeitsplätze verhindern	30
Vererbungsausschluss: Festlegen widersprechender Rollen	31
Zuweisung von Identitäten an mehrere Geschäftsrollen einschränken	32
Basisdaten für Geschäftsrollen	33
Rollenklassen für Geschäftsrollen	35
Rollentypen an Rollenklassen zuweisen	36
Rollentypen für Geschäftsrollen	37
Rollentypen erstellen und bearbeiten	38
Rollenklassen an Rollentypen zuweisen	39

Unternehmensbereiche für Geschäftsrollen	39
Attestierer	41
Genehmiger und Genehmiger (IT)	42
Geschäftsrollen erstellen und bearbeiten	43
Allgemeine Stammdaten für Geschäftsrollen	44
Adressinformationen für Geschäftsrollen	46
Unternehmensbereiche und Risikobewertung für Geschäftsrollen	47
Benutzerdefinierte Stammdaten für Geschäftsrollen	48
Identitäten, Geräte und Arbeitsplätze an Geschäftsrollen zuweisen	49
Unternehmensressourcen an Geschäftsrollen zuweisen	49
Analyse von Rollenmitgliedschaften und Zuweisungen an Identitäten	52
IT Betriebsdaten für Geschäftsrollen einrichten	54
IT Betriebsdaten ändern	58
Dynamische Rollen für Geschäftsrollen erstellen	59
Abteilungen, Kostenstellen und Standorte an Geschäftsrollen zuweisen	60
Vererbungsausschluss für Geschäftsrollen festlegen	60
Zusatzeigenschaften an Geschäftsrollen zuweisen	61
Zuweisungsressourcen für Geschäftsrollen erzeugen	62
Dynamische Rollen für Geschäftsrollen mit fehlerhaft ausgeschlossenen Identitäten	62
Zertifizierung von Geschäftsrollen	63
Berichte über Geschäftsrollen	64
Role Mining im One Identity Manager	66
Clusteranalyse als Grundlage des Role Mining	67
Arbeiten mit dem Programm Analyzer	68
Menüeinträge des Analyzers	68
Programmeinstellungen des Analyzers	69
Durchführen einer Analyse im Analyzer	69
Analysedaten mit dem Assistenten auswählen	70
Vordefinierte Analysen ausführen	73
Auswertung der Analyse	74
Änderungen aus der Analyse übernehmen	76
Über uns	78
Kontaktieren Sie uns	78
Technische Supportressourcen	78

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 in Microsoft Entra ID Mandanten. Identitäten können als Mitglieder in die einzelnen Geschäftsrollen aufgenommen werden. Bei entsprechender Konfiguration des One Identity Manager erhalten die Identitäten über diese Zuordnungen ihre Unternehmensressourcen.

HINWEIS: Voraussetzung für die Verwaltung von Geschäftsrollen im One Identity Manager ist die Installation des Geschäftsrollenmoduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch*.

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.

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

One Identity Manager Benutzer für Geschäftsrollen

In die Verwaltung von Geschäftsrollen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Administratoren für Geschäftsrollen	<p>Die Administratoren müssen der Anwendungsrolle Identity Management Geschäftsrollen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Erstellen und Bearbeiten die Geschäftsrollen.• Weisen Unternehmensressourcen an die Geschäftsrollen zu.• Attestieren die Stammdaten von Geschäftsrollen.• Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer.• Richten bei Bedarf weitere Anwendungsrollen ein.
Attestierer für Geschäftsrollen	<p>Die Attestierer müssen der Anwendungsrolle Identity Management Geschäftsrollen Attestierer oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Geschäftsrollen, für die sie verantwortlich sind.• Können die Stammdaten der Geschäftsrollen sehen, aber nicht bearbeiten. <p>HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.</p>
Genehmiger für Geschäftsrollen	<p>Die Genehmiger müssen der Anwendungsrolle Identity Management Geschäftsrollen Genehmiger oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Sind Genehmiger für den IT Shop.• Entscheiden über Bestellungen aus Geschäftsrollen, für die sie verantwortlich sind.
Genehmiger (IT) für	Die IT Genehmiger müssen der Anwendungsrolle Identity

Benutzer	Aufgaben
Geschäftsrollen	<p>Management Geschäftsrollen Genehmiger (IT) oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Sind IT Genehmiger für den IT Shop. • Entscheiden über Bestellungen aus Geschäftsrollen, für die sie verantwortlich sind.
One Identity Manager Administratoren	<p>One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen.</p> <p>One Identity Manager Administratoren:</p> <ul style="list-style-type: none"> • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Zusätzliche Manager	<p>Die zusätzlichen Manager müssen der Anwendungsrolle Identity Management Geschäftsrollen Zusätzliche Manager oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Sind berechtigt Geschäftsrollen zu verwalten.

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 Identität, 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.

Verwandte Themen

- [Vererbungsrichtungen innerhalb einer Hierarchie](#) auf Seite 9
- [Unterbrechen der Vererbung](#) auf Seite 11

Vererbungsrichtungen innerhalb einer Hierarchie

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

- Top-Down-Vererbung

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

- Bottom-Up-Vererbung

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

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

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

Beispiel: Zuweisung von Unternehmensressourcen über Top-Down-Vererbung

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

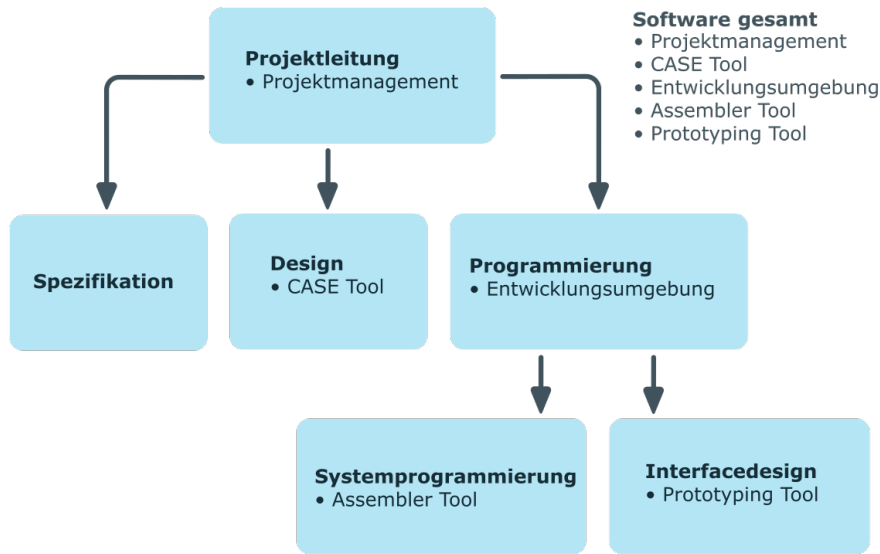
Abbildung 1: Zuweisung über Top-Down-Vererbung



Beispiel: Zuweisung von Unternehmensressourcen über Bottom-Up-Vererbung

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

Abbildung 2: Zuweisung über Bottom-Up-Vererbung



Unterbrechen der Vererbung

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

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

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

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

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

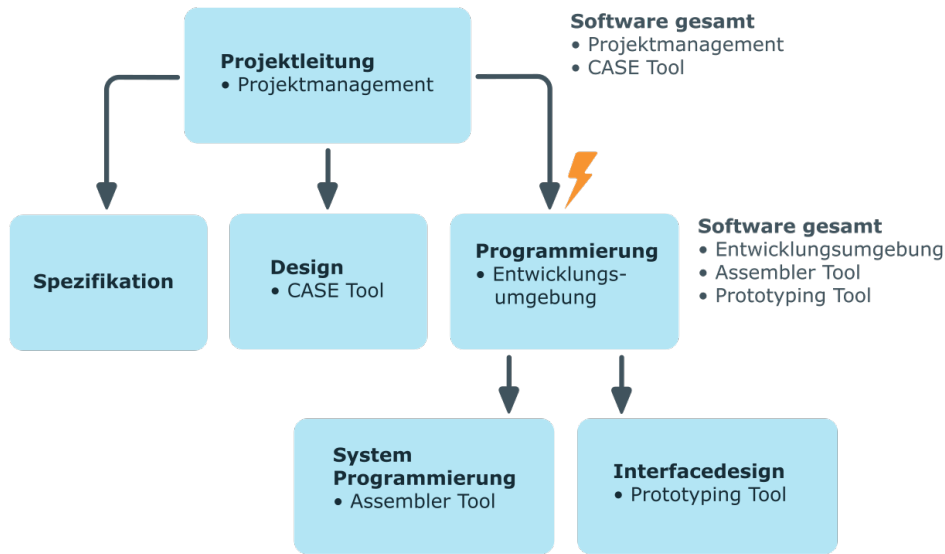
Abbildung 3: Unterbrechung der Vererbung in einer Top-Down-Vererbung



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

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

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



Verwandte Themen

- [Vererbung über Geschäftsrollen blockieren](#) auf Seite 29

Grundlagen zur Zuweisung von Unternehmensressourcen

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

Die Zuweisungsarten sind:

- [Direkte Zuweisung von Unternehmensressourcen](#)
- [Indirekte Zuweisung von Unternehmensressourcen](#)
- [Zuweisung von Unternehmensressourcen über dynamische Rollen](#)
- [Zuweisung von Unternehmensressourcen über IT Shop Bestellungen](#)

Direkte Zuweisung von Unternehmensressourcen

Die direkte Zuweisung von Unternehmensressourcen erfolgt beispielsweise durch die Zuordnung einer Unternehmensressource zu einer Identität, 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 Identität



Indirekte Zuweisung von Unternehmensressourcen

Bei der indirekten Zuweisung von Unternehmensressourcen werden Identitäten, 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 Identität, 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 Identität

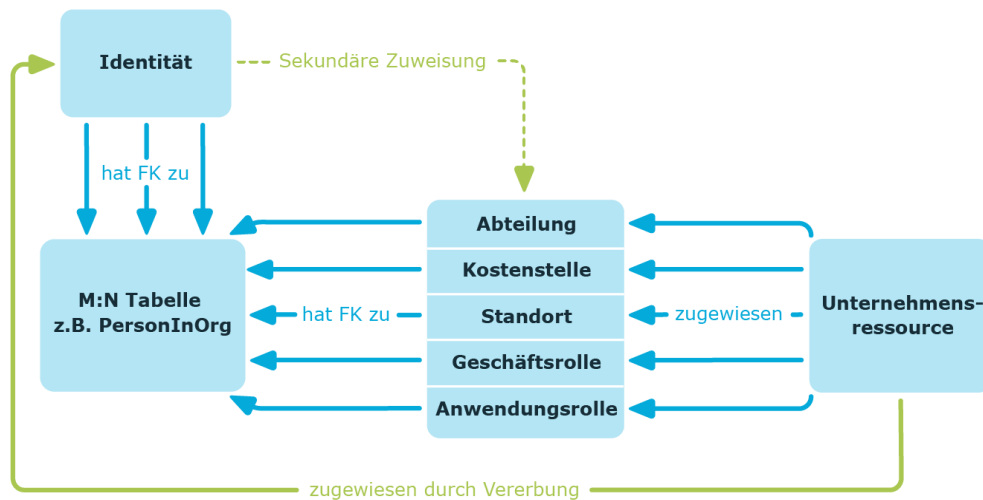


Sekundäre Zuweisung von Unternehmensressourcen

Die sekundäre Zuweisung erfolgt über die Einordnung einer Identität, 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 Identitäten, Geräte und Arbeitsplätze möglich ist, legen Sie an den Rollenklassen fest.

Abbildung 7: Schema einer sekundären Zuweisung



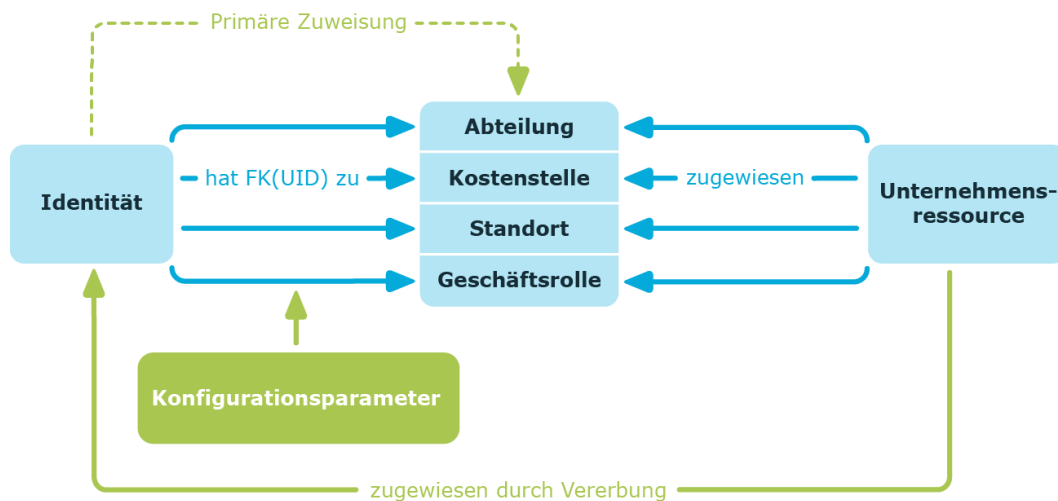
Verwandte Themen

- [Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben](#) auf Seite 27

Primäre Zuweisung von Unternehmensressourcen

Die primäre Zuweisung erfolgt über die Fremdschlüssel-Referenzierung einer Geschäftsrolle in den Identitäten-, Geräte- und Arbeitsplatzobjekten. Dazu nutzen Sie die Eingabefelder für Rollen auf den Stammdatenformularen für Identitäten, Geräte und Arbeitsplätze. Die Vererbung über die primären Zuweisungen kann über Konfigurationsparameter aktiviert werden. Für Identitäten 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	Identitäten können über primäre Zuweisung erben.
QER Structures Inherite Person FromOrg	Identitäten 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 von Unternehmensressourcen über dynamische Rollen

Die Zuweisung über dynamische Rollen ist ein Spezialfall der indirekten Zuweisung. Dynamische Rollen werden eingesetzt, um Rollenmitgliedschaften dynamisch festzulegen.

Dabei werden Identitäten, Geräte oder Arbeitsplätze nicht fest an eine Rolle zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen. Welche Identitäten, Geräte oder Arbeitsplätze diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Identitäten einer Geschäftsrolle zugewiesen werden; verlässt eine Identität diese Geschäftsrolle, verliert sie sofort die zugewiesenen Unternehmensressourcen.

Zuweisung von Unternehmensressourcen über IT Shop Bestellungen

Die Zuweisung über IT Shop Bestellungen ist ein Spezialfall der indirekten Zuweisung. Damit Unternehmensressourcen über IT Shop Bestellungen zugewiesen werden können, werden Identitäten 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 Identitäten zugewiesen. Neben den Unternehmensressourcen können über den IT Shop auch Rollenmitgliedschaften bestellt werden.

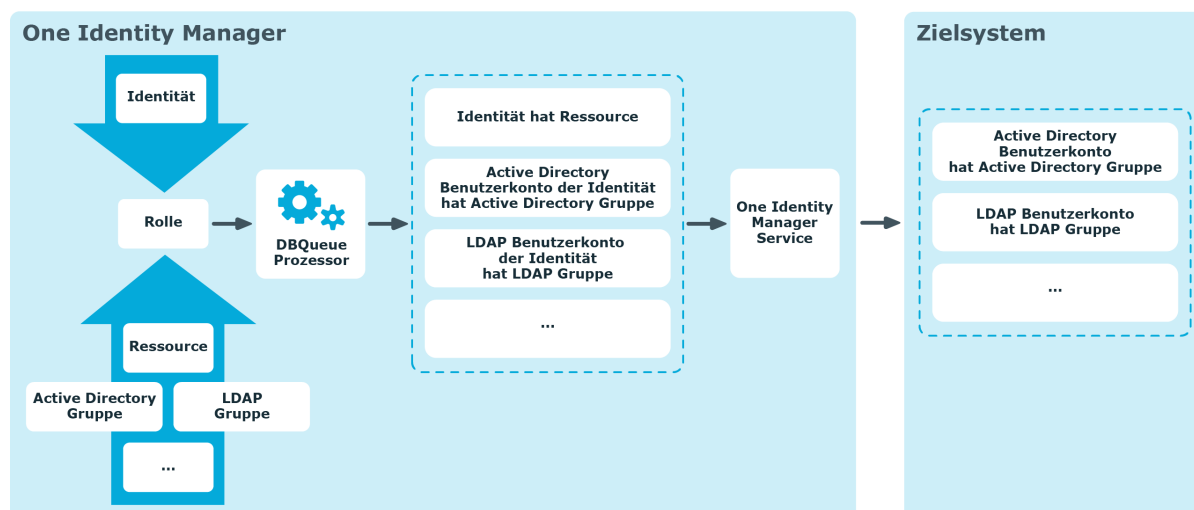
Abbildung 9: Schema einer Zuweisung über Bestellungen



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

Identitäten, 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:

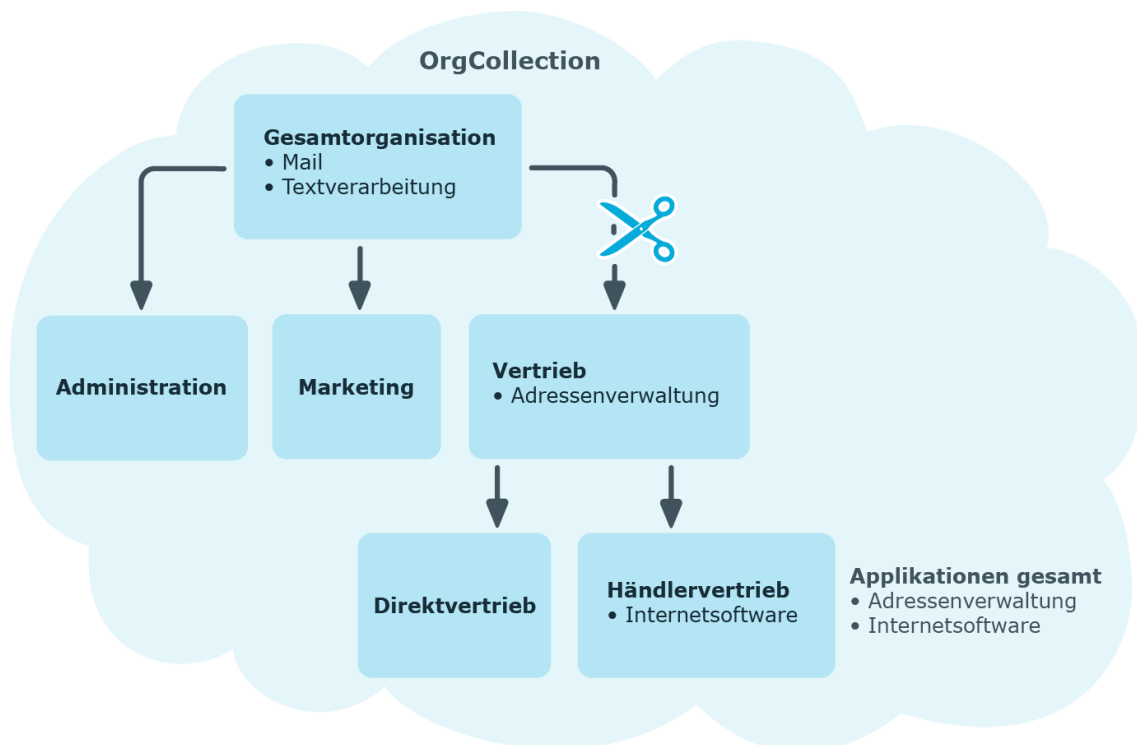
- UID_Org ist die Rolle, die erbt.
- UID_ParentOrg ist die Rolle, die vererbt.

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 Software an eine übergeordnete Rolle zugewiesen, werden die Mitglieder der Tabelle BaseTreeHasApp neu berechnet.

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

Berechnung der Zuweisungen

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

Es bedeuten:

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

Tabelle 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.

Bit 3	Bit 2	Bit 1	Bit 0	Wert in XOrigin	Bedeutung
1	1	0	1	13	Zuweisungsbestellung, direkt und über dynamische Rolle zugewiesen.
1	1	1	0	14	Zuweisungsbestellung, indirekt und über dynamische Rolle zugewiesen.
1	1	1	1	15	Zuweisungsbestellung, direkt, indirekt und über dynamische Rolle zugewiesen.

Besonderheiten bei Vererbung von Zuweisungen über Rollenhierarchie

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

Beispiel:

Für die Geschäftsrolle "Sales" wurde die Zuweisung einer Active Directory Gruppe bestellt. Die untergeordnete Geschäftsrolle "Sales EMEA" erbt diese Zuweisung. In der Tabelle OrgHasADSGroup ist XOrigin folgendermaßen gesetzt:

- Geschäftsrolle "Sales": XOrigin='8' (Zuweisungsbestellung)
- Geschäftsrolle "Sales EMEA": XOrigin='2' (indirekt zugewiesen)

Wirksamkeit von Zuweisungen

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

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

Vorbereiten der 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 Identitäten, 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 Identitäten, 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 Identitäten, Geräte oder Arbeitsplätze in Rollen aufgenommen werden, die sich ausschließende Unternehmensressourcen enthalten.

Detaillierte Informationen zum Thema

- [Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben](#) auf Seite 27
- [Festlegen der Vererbungsrichtung](#) auf Seite 28
- [Vererbung über Geschäftsrollen blockieren](#) auf Seite 29
- [Vererbung an Identitäten, Geräte oder Arbeitsplätze für einzelne Geschäftsrollen verhindern](#) auf Seite 29
- [Vererbung an einzelne Identitäten, Geräte oder Arbeitsplätze verhindern](#) auf Seite 30
- [Vererbungsausschluss für Geschäftsrollen festlegen](#) auf Seite 60
- [Zuweisung von Identitäten an mehrere Geschäftsrollen einschränken](#) auf Seite 32

Mögliche Zuweisungen von Unternehmensressourcen über Geschäftsrollen

Identitäten, Geräte und Arbeitsplätze können über indirekte Zuweisung Unternehmensressourcen erhalten. Dazu sind Identitäten, Geräte und Arbeitsplätze in beliebig viele Rollen eingeordnet. Über definierte Regeln erhalten die Identitäten, 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 Identitäten, 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	
	Identitäten	Arbeitsplätze
Ressourcen	möglich	-
Kontendefinitionen	möglich	-
Gruppen kundendefinierter Zielsysteme	möglich (Zuweisung an alle Benutzerkonten kundendefinierter Zielsysteme einer Identität, für welche die Vererbung von Gruppen zugelassen ist)	-
Systemberechtigungen kundendefinierter Zielsysteme	möglich (Zuweisung an alle Benutzerkonten kundendefinierter Zielsysteme einer Identität, für welche die Vererbung von Systemberechtigungen zugelassen ist)	-
Active Directory Gruppen	möglich (Zuweisung an alle Active Directory Benutzerkonten und Active Directory Kontakte einer Identität, für welche die Vererbung von Active Directory Gruppen zugelassen ist)	-
SharePoint Gruppen	möglich (Zuweisung an alle SharePoint Benutzerkonten einer Identität, für welche die Vererbung von SharePoint Gruppen zugelassen ist)	-
SharePoint Rollen	möglich (Zuweisung an alle SharePoint Benutzerkonten einer Identität, für welche die Vererbung von SharePoint Rollen zugelassen ist)	-
LDAP Gruppen	möglich (Zuweisung an alle LDAP Benutzerkonten einer Identität, für welche die Vererbung von LDAP	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Identitäten	Arbeitsplätze
	Gruppen zugelassen ist)	
Notes Gruppen	möglich (Zuweisung an alle Notes Benutzerkonten einer Identität, für welche die Vererbung von Notes Gruppen zugelassen ist)	-
SAP Gruppen	möglich (Zuweisung an alle SAP Benutzerkonten einer Identität, die im selben SAP Mandanten liegen und für welche die Vererbung von SAP Gruppen zugelassen ist)	-
SAP Profile	möglich (Zuweisung an alle SAP Benutzerkonten einer Identität, die im selben SAP Mandanten liegen und für welche die Vererbung von SAP Profilen zugelassen ist)	-
SAP Rollen	möglich (Zuweisung an alle SAP Benutzerkonten einer Identität, die im selben SAP Mandanten liegen und für welche die Vererbung von SAP Rollen zugelassen ist)	-
SAP Parameter	möglich (Zuweisung an alle SAP Benutzerkonten einer Identität, die im selben SAP System liegen)	-
Strukturelle Profile	möglich (Zuweisung an alle SAP Benutzerkonten einer Identität, die im selben SAP Mandanten liegen und für welche die Vererbung von strukturellen Profilen zugelassen ist)	-
BI Analyseberechtigungen	möglich (Zuweisung an alle BI Benutzerkonten einer Identität, die im selben System liegen und für welche die Vererbung von Gruppen zugelassen ist)	-
Microsoft Entra ID Gruppen	möglich (Zuweisung an alle Microsoft Entra ID Benutzerkonten einer Identität, für welche die Vererbung von Microsoft Entra ID Gruppen zugelassen ist)	-
Microsoft Entra ID Adminis-	möglich (Zuweisung an alle Microsoft	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Identitäten	Arbeitsplätze
tratorrollen	Entra ID Benutzerkonten einer Identität, für welche die Vererbung von Microsoft Entra ID Administratorrollen zugelassen ist)	
Microsoft Entra ID Abonnements	möglich (Zuweisung an alle Microsoft Entra ID Benutzerkonten einer Identität, für welche die Vererbung von Microsoft Entra ID Abonnements zugelassen ist)	-
Unwirksame Microsoft Entra ID Dienstpläne	möglich (Zuweisung an alle Microsoft Entra ID Benutzerkonten einer Identität, für welche die Vererbung von unwirksamen Microsoft Entra ID Dienstplänen zugelassen ist)	-
Cloud Gruppen	möglich (Zuweisung an alle Cloud Benutzerkonten einer Identität, für welche die Vererbung von Cloud Gruppen zugelassen ist)	-
Cloud Systemberechtigungen	möglich (Zuweisung an alle Cloud Benutzerkonten einer Identität, für welche die Vererbung von Cloud Systemberechtigungen zugelassen ist)	-
Unix Gruppen	möglich (Zuweisung an alle Unix Benutzerkonten einer Identität, für welche die Vererbung von Unix Gruppen zugelassen ist)	-
E-Business Suite Berechtigungen	möglich (Zuweisung an alle E-Business Suite Benutzerkonten einer Identität, die im selben E-Business Suite System liegen und für welche die Vererbung von E-Business Suite Gruppen zugelassen ist)	-
PAM Benutzergruppen	möglich (Zuweisung an alle PAM Benutzerkonten einer Identität, für welche die Vererbung von PAM Gruppen zugelassen ist)	-
Google Workspace Produkte	möglich (Zuweisung an alle	-

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Identitäten	Arbeitsplätze
und SKUs	Google Workspace Benutzerkonten einer Identität, die in der selben Kunden-Umgebung liegen und für welche die Vererbung von Google Workspace Produkten und SKUs zugelassen ist)	
Google Workspace Gruppen	möglich (Zuweisung an alle Google Workspace Benutzerkonten einer Identität, die in der selben Kunden-Umgebung liegen und für welche die Vererbung von Google Workspace Gruppen zugelassen ist)	-
SharePoint Online Gruppen	möglich (Zuweisung an alle SharePoint Online Benutzerkonten einer Identität, für welche die Vererbung von SharePoint Online Gruppen zugelassen ist)	-
SharePoint Online Rollen	möglich (Zuweisung an alle SharePoint Online Benutzerkonten einer Identität, für welche die Vererbung von SharePoint Online Rollen zugelassen ist)	-
Microsoft 365 Gruppen	möglich (Zuweisung an alle Microsoft Entra ID Benutzerkonten einer Identität, für welche die Vererbung von Microsoft 365 Gruppen zugelassen ist)	-
Exchange Online E-Mail-aktivierte Verteilergruppen	möglich (Zuweisung an alle an Exchange Online Postfächer, Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte einer Identität, für welche die Vererbung von Exchange Online E-Mail-aktivierten Verteilergruppen zugelassen ist)	-
OneLogin Rollen	möglich (Zuweisung an alle OneLogin Benutzerkonten einer Identität, für welche die Vererbung von OneLogin Rollen zugelassen ist)	

Zuweisbare Unternehmensressourcen	Mitglieder in Rollen	
	Identitäten	Arbeitsplätze
Systemrollen	möglich	möglich
Abonnierbare Berichte	möglich	-
Software	möglich	möglich

Verwandte Themen

- [Unternehmensressourcen an Geschäftsrollen zuweisen](#) auf Seite 49

Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben

Das Standardverfahren für die Zuweisung von Unternehmensressourcen über Rollen ist die sekundäre Zuweisung. Dafür werden sowohl Identitäten, 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 Identitäten im Manager direkt an Geschäftsrollen zuzuweisen, aktivieren Sie an der Rollenklasse **Geschäftsrolle**, für den Eintrag **Identitäten** die Optionen **Zuweisungen erlaubt** und **Direkte Zuweisungen erlaubt**.

Sollen Identitäten die Mitgliedschaft in einer Geschäftsrolle nur über den IT Shop erhalten, dann aktivieren Sie an der Rollenklasse **Geschäftsrolle**, für den Eintrag **Identitäten**, die Option **Zuweisungen erlaubt** und deaktivieren die Option **Direkte Zuweisungen erlaubt**. Im IT Shop muss dann eine entsprechende Zuweisungsressource verfügbar sein.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Geschäftsrollen > 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 9
- [Rollenklassen für Geschäftsrollen](#) auf Seite 35

Vererbung über Geschäftsrollen blockieren

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

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

Um die Vererbung für Geschäftsrollen zu unterbrechen

1. Wählen Sie im Manager in der Kategorie **Geschäftsrollen** die Geschäftsrolle.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Aktivieren Sie die Option **Vererbung blockieren**.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Unterbrechen der Vererbung](#) auf Seite 11
- [Vererbung an Identitäten, Geräte oder Arbeitsplätze für einzelne Geschäftsrollen verhindern](#) auf Seite 29
- [Vererbung an einzelne Identitäten, Geräte oder Arbeitsplätze verhindern](#) auf Seite 30

Vererbung an Identitäten, Geräte oder Arbeitsplätze für einzelne Geschäftsrollen verhindern

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

Um die Vererbung für Geschäftsrollen zu verhindern

1. Wählen Sie im Manager in der Kategorie **Geschäftsrollen** die Geschäftsrolle.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

3. Aktivieren Sie eine oder mehrere der folgenden Optionen.
 - Um die Vererbung an Identitäten zu verhindern, aktivieren Sie die Option **Keine Vererbung an Identitäten**.
 - Um die Vererbung an Geräte zu verhindern, aktivieren Sie die Option **Keine Vererbung an Geräte**.
 - Um die Vererbung an Arbeitsplätze zu verhindern, aktivieren Sie die Option **Keine Vererbung an Arbeitsplätze**.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Vererbung über Geschäftsrollen blockieren](#) auf Seite 29
- [Vererbung an einzelne Identitäten, Geräte oder Arbeitsplätze verhindern](#) auf Seite 30

Vererbung an einzelne Identitäten, Geräte oder Arbeitsplätze verhindern

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

Um die Vererbung für eine Identität zu verhindern

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

Die Identität erbt keine Unternehmensressourcen über Rollen.

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

4. Speichern Sie die Änderungen.

Um die Vererbung für ein Gerät zu verhindern

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

Das Gerät erbt keine Unternehmensressourcen über Rollen.

HINWEIS: Diese Option hat keinen Einfluss auf direkte Zuweisungen! Direkt

- | zugewiesene Unternehmensressourcen bleiben zugewiesen.
4. Speichern Sie die Änderungen.

Um die Vererbung für einen Arbeitsplatz zu verhindern

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

Der Arbeitsplatz erbt keine Unternehmensressourcen über Rollen.

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

4. Speichern Sie die Änderungen.

Verwandte Themen

- [Vererbung über Geschäftsrollen blockieren](#) auf Seite 29
- [Vererbung an Identitäten, Geräte oder Arbeitsplätze für einzelne Geschäftsrollen verhindern](#) auf Seite 29

Vererbungsausschluss: Festlegen widersprechender Rollen

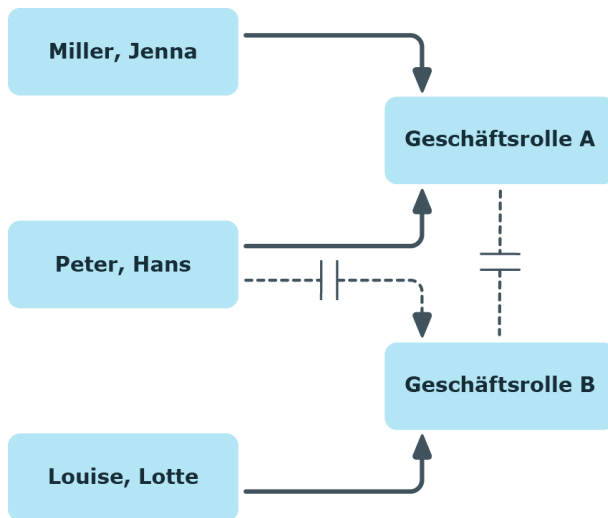
Um zu verhindern, dass Identitäten, Geräte oder Arbeitsplätze gleichzeitig an verschiedene Rollen zugewiesen werden und über diese Rollen sich ausschließende Unternehmensressourcen erhalten könnten, können Sie widersprechende Rollen definieren. Dabei legen Sie fest, welche Geschäftsrollen sich gegenseitig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

| **HINWEIS:** Nur Rollen, die direkt als widersprechende Rollen definiert sind, können nicht an ein und dieselbe Identität (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.

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

Verwandte Themen

- [Vererbungsausschluss für Geschäftsrollen festlegen](#) auf Seite 60

Zuweisung von Identitäten an mehrere Geschäftsrollen einschränken

Unter Umständen ist es erforderlich, dass eine Identität nur an eine Geschäftsrolle zugewiesen werden kann, beispielsweise innerhalb einer Projektstruktur.

Um dieses Verhalten abzubilden, können Sie die Option **Keine Mehrfachzuweisung von Identitäten** nutzen. Die Option können Sie für Rollenklassen und Rollentypen aktivieren.

- Ist die Option für eine Rollenklasse aktiviert, kann eine Identität nur einer Geschäftsrolle dieser Rollenklasse zugewiesen werden. Eine Zuweisung der Identität an andere Geschäftsrollen, die zu dieser Rollenklasse gehören, wird abgelehnt.
- Ist die Option für einen Rollentyp aktiviert, kann eine Identität nur an eine Geschäftsrolle dieses Rollentyps zugewiesen werden. Eine Zuweisung der Identität an andere Geschäftsrollen, die zu diesem Rollentyp gehören, wird abgelehnt.

HINWEIS:

- Die Überprüfung erfolgt nur für direkte Zuweisungen von Identitäten zu Geschäftsrollen.
- Nutzen Sie die Konsistenzprüfungen **Mehrere Rollenzuweisungen trotz IsPersonAssignOnce an OrgRoot** und **Mehrere Rollenzuweisungen trotz IsPersonAssignOnce an OrgType**, um unzulässige Zuweisungen zu Geschäftsrollen zu ermitteln. Diese Zuweisungen können beispielsweise über dynamische Rollen oder durch Bestellungen entstanden sein. Ausführliche Informationen zu Konsistenzprüfungen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
- Wenn eine Identität bereits an mehrere Geschäftsrollen einer Rollenklasse oder eines Rollentyps zugewiesen wurde, dann kann die Option nicht mehr für diese Rollenklasse oder für diesen Rollentyp gesetzt werden.

Verwandte Themen

- [Rollenklassen für Geschäftsrollen](#) auf Seite 35
- [Rollentypen für Geschäftsrollen](#) auf Seite 37

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

- Attestierer

Im One Identity Manager können Sie an Geschäftsrollen Identitäten 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. Ausführliche Informationen zur Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

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

- Genehmiger und Genehmiger (IT)

Im One Identity Manager können Sie an Geschäftsrollen Identitäten 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. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

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

Detaillierte Informationen zum Thema


- [Rollenklassen für Geschäftsrollen](#) auf Seite 35
- [Rollentypen für Geschäftsrollen](#) auf Seite 37
- [Unternehmensbereiche für Geschäftsrollen](#) auf Seite 39

- [Attestierer](#) auf Seite 41
- [Genehmiger und Genehmiger \(IT\)](#) auf Seite 42

Rollenklassen für Geschäftsrollen



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. Erlauben Sie für die Rollenklassen die Zuweisungen von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen.

Um Rollenklassen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen**.
2. Wählen Sie in der Ergebnisliste die Rollenklasse und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- 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 im Manager angezeigt. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
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	Vererbungsrichtung Bottom-Up.

Eigenschaft	Beschreibung
nach oben	
Delegierbar	Gibt an, ob die Mitgliedschaften in den Rollen dieser Rollenklasse delegiert werden können.
Zuweisungen erlaubt	Gibt an, ob die Zuweisung der jeweiligen Objekttypen zu Rollen der Rollenklasse generell erlaubt ist. Konfigurieren Sie die erlaubten Zuweisungen im Manager über die Aufgabe Rollenzuweisungen konfigurieren .
Direkte Zuweisungen erlaubt	Gibt an, ob die jeweiligen Objekttypen direkt an die Rollen der Rollenklasse zugewiesen werden kann. Konfigurieren Sie die erlaubten Zuweisungen im Manager über die Aufgabe Rollenzuweisungen konfigurieren .
Keine Mehrfachzuweisung von Identitäten	Gibt an, ob eine Identität nur einer Geschäftsrolle dieser Rollenklasse zugewiesen werden. Ist die Option für eine Rollenklasse aktiviert, kann eine Identität nur einer Geschäftsrolle dieser Rollenklasse zugewiesen werden. Eine Zuweisung der Identität an andere Geschäftsrollen, die zu dieser Rollenklasse gehören, wird abgelehnt.

Verwandte Themen

- [Vererbungsrichtungen innerhalb einer Hierarchie](#) auf Seite 9
- [Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben](#) auf Seite 27

Rollentypen an Rollenklassen zuweisen


Zur weiteren Klassifizierung können Sie Rollentypen definieren und an Rollenklassen zuweisen. Beachten Sie die unter [Rollentypen für Geschäftsrollen](#) auf Seite 37 genannten Einschränkungen.

Um Rollentypen an eine Rollenklasse zuzuweisen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie den Rollentyp und doppelklicken Sie .

Verwandte Themen

- [Rollentypen für Geschäftsrollen](#) auf Seite 37
- [Rollentypen erstellen und bearbeiten](#) auf Seite 38
- [Rollenklassen an Rollentypen zuweisen](#) auf Seite 39

Rollentypen für Geschäftsrollen

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

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

Beispiel:

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

- Der Rollenklasse **Externe Projekte** wird der Rollentyp **Geschäftsrollen** zugewiesen.
Rollen dieser Rollenklasse können den Rollentyp **Geschäftsrollen** erhalten.
- Der Rollenklasse **Mitarbeiter** werden die Rollentypen **Geschäftsrolle**, **Region** und **Land** zugewiesen.
Rollen diese Rollenklasse können die Rollentypen **Geschäftsrolle**, **Region** und **Land** erhalten.
- Der Rollenklasse **Standort** werden die Rollentypen **Region** und **Land** zugewiesen.
Standorte können die Rollentypen **Region** und **Land** erhalten.

- Den Rollenklassen **Kostenstelle** und **Abteilung** werden keine Rollentypen zugewiesen.
Kostenstellen und Abteilungen können die Rollentypen **Vertrieb** und **Entwicklung** erhalten.



Verwandte Themen

- [Rollentypen erstellen und bearbeiten](#) auf Seite 38
- [Rollenklassen an Rollentypen zuweisen](#) auf Seite 39
- [Rollentypen an Rollenklassen zuweisen](#) auf Seite 36

Rollentypen erstellen und bearbeiten

Zur weiteren Klassifizierung können Sie Rollentypen erstellen und bearbeiten. Standardrollentypen können Sie nicht bearbeiten.

Um Rollentypen zu erstellen

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollentypen**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die folgenden Informationen:
 - **Rollentyp**: Bezeichnung des Rollentyp. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
 - **Beschreibung**: (Optional) Freitextfeld für zusätzliche Erläuterungen.
 - **Keine Mehrfachzuweisung von Identitäten**: Gibt an, ob eine Identität nur einer Geschäftsrolle dieses Rollentyps zugewiesen werden. Ist die Option für einen Rollentyp aktiviert, kann eine Identität nur an eine Geschäftsrolle dieses Rollentyps zugewiesen werden. Eine Zuweisung der Identität an andere Geschäftsrollen, die zu diesem Rollentyp gehören, wird abgelehnt.

HINWEIS: Die Option wirkt nicht für Abteilungen, Kostenstellen und Standorte.

4. Speichern Sie die Änderungen.

Um Rollentypen zu erstellen

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

4. Bearbeiten Sie die Stammdaten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Rollenklassen an Rollentypen zuweisen](#) auf Seite 39
- [Rollentypen an Rollenklassen zuweisen](#) auf Seite 36

Rollenklassen an Rollentypen zuweisen


Zur weiteren Klassifizierung können Sie Rollentypen definieren und an Rollenklassen zuweisen. Beachten Sie die unter [Rollentypen für Geschäftsrollen](#) auf Seite 37 genannten Einschränkungen.

Um Rollenklassen an einen Rollentyp zuzuweisen

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

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

Um eine Zuweisung zu entfernen

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

Verwandte Themen

- [Rollentypen für Geschäftsrollen](#) auf Seite 37
- [Rollentypen erstellen und bearbeiten](#) auf Seite 38
- [Rollentypen an Rollenklassen zuweisen](#) auf Seite 36

Unternehmensbereiche für Geschäftsrollen

Um Regelprüfungen im Rahmen des Identity Audit für verschiedene Bereiche Ihres Unternehmens auswerten zu können, richten Sie Unternehmensbereiche ein. Unternehmensbereiche können an hierarchische Rollen, Complainceregeln, SAP Funktionen und Leistungspositionen zugeordnet werden. Für die Unternehmensbereiche und die hierarchischen Rollen können Sie Kriterien erfassen, die Auskunft über das Risiko

von Regelverletzungen geben. Für die Bewertung der Risiken legen Sie fest, wie viele Regelverletzungen in einem Unternehmensbereich oder einer Rolle zulässig sind. Für jede Rolle können Sie separate Bewertungskriterien erfassen, wie beispielsweise Risikoindex oder Transparenzindex.


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

Beispiel: Einsatz von Unternehmensbereichen

Das Risiko von Regelverletzungen für 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. Legen Sie die Anzahl zulässiger Regelverletzungen für die Unternehmensbereiche fest.
5. Weisen Sie die Unternehmensbereiche den Complianceregeln zu, die für die Auswertung relevant sind.
6. Erstellen Sie über die Berichtsfunktion des One Identity Manager einen Bericht, der das Ergebnis der Regelprüfung für die Unternehmensbereiche nach beliebigen Kriterien aufbereitet.

Um Unternehmensbereiche zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Unternehmensbereiche**.
2. Wählen Sie in der Ergebnisliste einen Unternehmensbereich und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- ODER -
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Unternehmensbereichs.
4. Speichern Sie die Änderungen.

Für einen Unternehmensbereich erfassen Sie folgende Stammdaten.

Tabelle 7: Eigenschaften von Unternehmensbereichen

Eigenschaft	Beschreibung
Unternehmensbereich	Bezeichnung des Unternehmensbereichs.
Überg. Unternehmensbereich	Übergeordneter Unternehmensbereich in einer Hierarchie.

Eigenschaft	Beschreibung
	Wählen Sie aus der Auswahlliste den übergeordneten Unternehmensbereich aus, um Unternehmensbereiche hierarchisch zu organisieren.
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in diesem Unternehmensbereich zulässig sind. Dieser Wert kann bei der Regelprüfung ausgewertet werden. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Complianceregeln vorhanden ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- *One Identity Manager Administrationshandbuch für Complianceregeln*

Attestierer

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

Im One Identity Manager können Sie an Geschäftsrollen Identitäten 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. Ausführliche Informationen zur Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

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

Tabelle 8: 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: <ul style="list-style-type: none"> • Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Geschäftsrollen, für die sie verantwortlich sind. • Können die Stammdaten der Geschäftsrollen sehen, aber nicht bearbeiten.

Benutzer	Aufgaben
----------	----------


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

Um Identitäten in die Standardanwendungsrolle für Attestierer aufzunehmen

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

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

Um eine Zuweisung zu entfernen

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

Genehmiger und Genehmiger (IT)

Im One Identity Manager können Sie an Geschäftsrollen Identitäten 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. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

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

Tabelle 9: 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: <ul style="list-style-type: none">• Sind Genehmiger für den IT Shop.• Entscheiden über Bestellungen aus Geschäftsrollen, für die sie verantwortlich sind.
Genehmiger (IT)	Die IT Genehmiger müssen der Anwendungsrolle Identity


Benutzer	Aufgaben
für Geschäftsrollen	<p>Management Geschäftsrollen Genehmiger (IT) oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • 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 im Manager die Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Genehmiger**.
- ODER -
Wählen Sie im Manager die Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Genehmiger (IT)**.
2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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


Um eine Zuweisung zu entfernen

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

Geschäftsrollen erstellen und 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.

Um Geschäftsrollen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- ODER -
Klicken Sie in der Ergebnisliste .

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





Verwandte Themen




- [Rollenklassen für Geschäftsrollen](#) auf Seite 35

Allgemeine Stammdaten für Geschäftsrollen

Für eine Geschäftsrolle erfassen Sie die folgenden allgemeine Stammdaten.

Tabelle 10: Allgemeine Stammdaten einer Geschäftsrolle

Eigenschaft	Beschreibung
Geschäftsrolle	Bezeichnung der Geschäftsrolle. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
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 vorgelegt. 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.
Vollständiger Name	Kompletter Name der Geschäftsrollen einschließlich übergeordneter Geschäftsrollen. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
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.

Eigenschaft	Beschreibung
Genehmiger (IT)	<p>Anwendungsrolle, deren Mitglieder IT Shop-Bestellungen für Mitglieder dieser Geschäftsrolle entscheiden.</p> <p>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.</p>
Manager	Verantwortlicher Manager der Geschäftsrolle.
2. Verantwortlicher	Stellvertretender Manager der Geschäftsrolle.
Zusätzliche Manager	<p>Anwendungsrolle für eine Gruppe von Managern und Stellvertretern, die diese Geschäftsrolle verwalten.</p> <p>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.</p>
Attestierer	<p>Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge für die Geschäftsrolle zu entscheiden.</p> <p>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.</p> <p>HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.</p>
Abteilung	Abteilung, der die Geschäftsrolle primär zugeordnet ist.
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	<p>Zertifizierungsstatus der Geschäftsrolle. Folgende Zertifizierungsstatus können ausgewählt werden.</p> <ul style="list-style-type: none"> • 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. <p>Der Zertifizierungsstatus kann abhängig vom Ergebnis regelmäßiger Attestierungen gesetzt werden.</p>

Eigenschaft	Beschreibung
Datenquelle Import	Zielsystem beziehungsweise Datenquelle, aus welcher der Datensatz importiert wurde.
Vererbung blockieren	Gibt an, 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 Identitäten	Gibt an, ob die Vererbung an Identitäten für diese Geschäftsrolle vorübergehend verhindert werden soll.
Keine Vererbung an Geräte	Gibt an, ob die Vererbung an Geräte für diese Geschäftsrolle vorübergehend verhindert werden soll.
Keine Vererbung an Arbeitsplätze	Gibt an, ob die Vererbung an Arbeitsplätze für diese Geschäftsrolle vorübergehend verhindert werden soll.
Dynamische Rollen nicht erlaubt	Gibt an, ob für die Geschäftsrolle eine dynamische Rolle erstellt werden darf.

Verwandte Themen

- [Rollenklassen für Geschäftsrollen](#) auf Seite 35
- [Rollentypen für Geschäftsrollen](#) auf Seite 37
- [Genehmiger und Genehmiger \(IT\)](#) auf Seite 42
- [Attestierer](#) auf Seite 41
- [Vererbung an Identitäten, Geräte oder Arbeitsplätze für einzelne Geschäftsrollen verhindern](#) auf Seite 29
- [Dynamische Rollen für Geschäftsrollen erstellen](#) auf Seite 59
- [Zertifizierung von Geschäftsrollen](#) auf Seite 63

Adressinformationen für Geschäftsrollen

Erfassen Sie die folgenden Stammdaten zur Erreichbarkeit der Geschäftsrolle.

Tabelle 11: Adressdaten einer Geschäftsrolle

Eigenschaft	Beschreibung
Adresse	Postanschrift der Geschäftsrolle.
Straße	Straße.

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

Unternehmensbereiche und Risikobewertung für Geschäftsrollen

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

Tabelle 12: Stammdaten zum Unternehmensbereich einer Geschäftsrolle

Eigenschaft	Beschreibung
Unternehmensbereich	Unternehmensbereich der Abteilung. Die Angabe wird zur Risikobewertung der Abteilung benötigt.
Risikoindex (berechnet)	Für die Risikobewertung der Abteilung wird anhand der zugewiesenen Unternehmensressourcen ein Risikoindex berechnet. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen an den Standort

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

Verwandte Themen

- [Unternehmensbereiche für Geschäftsrollen](#) auf Seite 39

Benutzerdefinierte Stammdaten für Geschäftsrollen

Erfassen Sie benutzerdefinierte Stammdaten. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Tabelle 13: Benutzerdefinierte Stammdaten einer Bearbeitergruppe

Eigenschaft	Beschreibung
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen.
Freies Datum Nr.01 ... Freies Datum Nr.03	Zusätzliche unternehmensspezifische Informationen.

Identitäten, Geräte und Arbeitsplätze an Geschäftsrollen zuweisen

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


TIPP: Nutzen Sie dynamische Rollen, um Identitäten, Geräte und Arbeitsplätze automatisch an Geschäftsrollen zuzuweisen.

Um Identitäten, Geräte und Arbeitsplätze in eine Geschäftsrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die entsprechende Aufgabe.
 - **Identitäten zuweisen**
 - **Geräte zuweisen**
 - **Arbeitsplätze zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Objekte zu.

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

Um eine Zuweisung zu entfernen

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

Verwandte Themen

- [Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben](#) auf Seite 27
- [Unternehmensressourcen an Geschäftsrollen zuweisen](#) auf Seite 49
- [Dynamische Rollen für Geschäftsrollen erstellen](#) auf Seite 59

Unternehmensressourcen an Geschäftsrollen zuweisen

Das Standardverfahren für die Zuweisung von Unternehmensressourcen an Identitäten, Geräte und Arbeitsplätze ist die indirekte Zuweisung. Dabei wird eine Identität, 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 Identität, ein Gerät oder einen Arbeitsplatz.

Die indirekte Zuweisung wird unterschieden in

- Sekundäre Zuweisung

Die sekundäre Zuweisung erfolgt über die Einordnung einer Identität, 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 Identität, 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 Identitäten-, Geräte- und Arbeitsplatzobjekten. Die Vererbung über die primären Zuweisungen kann über Konfigurationsparameter aktiviert werden.

Damit Unternehmensressourcen an Identitäten, 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

Unternehmensressource	Verfügbar im Modul
Ressourcen	immer
Kontendefinitionen	Zielsystem Basismodul
Gruppen kundendefinierter Zielsysteme	Zielsystem Basismodul
Systemberechtigungen kundendefinierter Zielsysteme	Zielsystem Basismodul
Active Directory Gruppen	Active Directory Modul
SharePoint Gruppen	SharePoint Modul
SharePoint Rollen	SharePoint Modul
LDAP Gruppen	LDAP Modul
Notes Gruppen	Domino Modul

Unternehmensressource	Verfügbar im Modul
SAP Gruppen	SAP R/3 Benutzermanagement-Modul
SAP Profile	SAP R/3 Benutzermanagement-Modul
SAP Rollen	SAP R/3 Benutzermanagement-Modul
SAP Parameter	SAP R/3 Benutzermanagement-Modul
Strukturelle Profile	Modul SAP R/3 Strukturelle Profile Add-on
BI Analyseberechtigungen	Modul SAP R/3 Analyseberechtigungen Add-on
E-Business Suite Berechtigungen	Oracle E-Business Suite Modul
Systemrollen	Systemrollenmodul
Abonnierbare Berichte	Modul Berichtsabonnement
Software	Modul Softwaremanagement
Microsoft Entra ID Gruppen	Microsoft Entra ID Modul
Microsoft Entra ID Administratorrollen	Microsoft Entra ID Modul
Microsoft Entra ID Abonnements	Microsoft Entra ID Modul
Unwirksame Microsoft Entra ID Dienstpläne	Microsoft Entra ID Modul
Microsoft Entra ID Rollenzuweisungen	Microsoft Entra ID Modul
Microsoft Entra ID Rollenberechtigungen	Microsoft Entra ID Modul
Unix Gruppen	Modul Unix-basierte Zielsysteme
Cloud Gruppen	Modul Cloud Systems Management
Cloud Systemberechtigungen	Modul Cloud Systems Management
PAM Benutzergruppen	Privileged Account Governance Modul
Google Workspace Gruppen	Google Workspace Modul
Google Workspace Produkte und SKUs	Google Workspace Modul
SharePoint Online Gruppen	SharePoint Online Modul
SharePoint Online Rollen	SharePoint Online Modul
OneLogin Rollen	OneLogin Modul


Um Unternehmensressourcen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **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.

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

Um eine Zuweisung zu entfernen

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

Detaillierte Informationen zum Thema

- [Grundlagen zur Zuweisung von Unternehmensressourcen](#) auf Seite 13
- [Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben](#) auf Seite 27

Verwandte Themen

- [Mögliche Zuweisungen von Unternehmensressourcen über Geschäftsrollen](#) auf Seite 22
- [Identitäten, Geräte und Arbeitsplätze an Geschäftsrollen zuweisen](#) auf Seite 49
- [Dynamische Rollen für Geschäftsrollen erstellen](#) auf Seite 59

Analyse von Rollenmitgliedschaften und Zuweisungen an Identitäten

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


Beispiele: Übersicht von Zuweisungen


- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese

Gruppe oder Systemberechtigung besitzen.

- Wird der Bericht für eine Compianceregeln erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese Compianceregeln verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Identitäten der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Identitäten der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

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







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

Abbildung 13: Symbolleiste des Berichts Übersicht aller Zuweisungen



Tabelle 15: Bedeutung der Symbole in der Symbolleiste des Berichtes

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

IT Betriebsdaten für Geschäftsrollen einrichten

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

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

Beispiel: Abbildung von IT Betriebsdaten

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

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

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

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

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

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

Um den Anwendungsbereich festzulegen

- Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.
 - Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder, für eine Kontendefinition, die Tabelle TSBAccountDef.
 - Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.
 - Klicken Sie **OK**.
- **Spalte:** Wählen Sie die Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.
In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript TSB_ITDataFromOrg verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
 - **Wert:** Erfassen Sie den konkreten Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

5. Speichern Sie die Änderungen.

IT Betriebsdaten für Zielsysteme

Die IT Betriebsdaten, die in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen oder Ändern von Benutzerkonten und Postfächer für eine Identität 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 16: Zielsystemtyp-abhängige IT Betriebsdaten

Zielsystemtyp	IT Betriebsdaten
Active Directory	Container Homeserver Profilservers Terminal Homeserver Terminal Profilservers Gruppen erbbbar Identitätstyp Privilegiertes Benutzerkonto Container für deaktivierte Benutzerkonten

Zielsystemtyp	IT Betriebsdaten
Microsoft Exchange	Postfachdatenbank
LDAP	Container Gruppen erbbbar Identitätstyp Privilegiertes Benutzerkonto
Domino	Server Zertifikat Vorlage der Postdatei Identitätstyp
SharePoint	Authentifizierungsmodus Gruppen erbbbar Rollen erbbbar Identitätstyp Privilegiertes Benutzerkonto
SharePoint Online	Gruppen erbbbar Rollen erbbbar Privilegiertes Benutzerkonto Authentifizierungsmodus
Kundendefinierte Zielsysteme	Container (je Zielsystem) Gruppen erbbbar Identitätstyp Privilegiertes Benutzerkonto
Microsoft Entra ID	Gruppen erbbbar Administratorrollen erbbbar Abonnements erbbbar Unwirksame Dienstpläne erbbbar Identitätstyp Privilegiertes Benutzerkonto Kennwort bei der nächsten Anmeldung ändern
Cloud Zielsystem	Container (je Zielsystem) Gruppen erbbbar Identitätstyp

Zielsystemtyp	IT Betriebsdaten
	Privilegiertes Benutzerkonto
Unix-basierte Zielsysteme	Login-Shell Gruppen erbbar Identitätstyp Privilegiertes Benutzerkonto
Oracle E-Business Suite	Identitätstyp Gruppen erbbar Privilegiertes Benutzerkonto
SAP R/3	Identitätstyp Gruppen erbbar Rollen erbbar Profile erbbar Strukturelle Profile erbbar Privilegiertes Benutzerkonto
Exchange Online	Gruppen erbbar
Privileged Account Management	Authentifizierungsanbieter Gruppen erbbar Identitätstyp Privilegiertes Benutzerkonto
Google Workspace	Organisation Gruppen erbbar Produkte und SKUs erbbar Admin-Rollen-Zuordnungen erbbar Identitätstyp Privilegiertes Benutzerkonto Kennwort bei der nächsten Anmeldung ändern
OneLogin	Rollen erbbar Identitätstyp Privilegiertes Benutzerkonto Lizenzierungsstatus OneLogin Gruppe

IT Betriebsdaten ändern

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

Voraussetzungen

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

HINWEIS: Ändert sich die Zuordnung einer Identität zu einer primären 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. Es bedeuten:

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

Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Dynamische Rollen für Geschäftsrollen erstellen

Über diese Aufgabe definieren Sie dynamische Rollen für einzelne Geschäftsrollen. Dynamische Rollen werden eingesetzt, um Rollenmitgliedschaften dynamisch festzulegen. Dabei werden Identitäten, Geräte oder Arbeitsplätze nicht fest an eine Rolle zugewiesen, sondern nur dann, wenn sie bestimmte Bedingungen erfüllen. Welche Identitäten (Geräte oder Arbeitsplätze) diese Bedingungen erfüllen, wird regelmäßig überprüft. Dadurch ändern sich die Rollenmitgliedschaften dynamisch. So können beispielsweise Unternehmensressourcen an alle Identitäten einer Geschäftsrolle zugewiesen werden; verlässt eine Identität diese Geschäftsrolle verliert sie sofort die zugewiesenen Unternehmensressourcen.

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

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

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

Um eine dynamische Rolle für eine Geschäftsrolle zu erstellen

1. Wählen Sie im Manager 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 im Manager die Kategorie **Geschäftsrollen** > **<Rollenklasse>** > **Dynamische Rollen**.
2. Wählen Sie in der Ergebnisliste eine Geschäftsrolle.
3. Öffnen Sie das Überblicksformular der Geschäftsrolle.
4. Klicken Sie im Formularelement **Dynamische Rollen** auf die Bezeichnung der dynamischen Rolle.
5. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
6. Bearbeiten Sie die Stammdaten der dynamische Rolle.
7. Speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten für Geschäftsrollen](#) auf Seite 44
- [Zuweisung von Identitäten, Geräten, Arbeitsplätzen und Unternehmensressourcen an Geschäftsrollen erlauben](#) auf Seite 27

Abteilungen, Kostenstellen und Standorte an Geschäftsrollen 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 im Manager 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.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten für Geschäftsrollen](#) auf Seite 44

Vererbungsausschluss für Geschäftsrollen festlegen

Um zu verhindern, dass Identitäten, 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 Identität (Gerät, Arbeitsplatz) zuweisen.

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

Um den Vererbungsausschluss zu konfigurieren

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

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

Um den Vererbungsausschluss für 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 31

Zusatzeigenschaften an Geschäftsrollen 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. Ausführliche Informationen zu Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln*.

Um Zusatzeigenschaften für eine Geschäftsrolle festzulegen

1. Wählen Sie im Manager 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Zuweisungsressourcen für Geschäftsrollen 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. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Um eine Zuweisungsressource auf eine Geschäftsrolle einzuschränken

1. Wählen Sie im Manager 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.

HINWEIS: Geschäftsrollen, die mit einer Zuweisungsressource verbunden sind, können erst gelöscht werden, wenn die zugehörige Zuweisungsressource gelöscht ist.

Dynamische Rollen für Geschäftsrollen mit fehlerhaft ausgeschlossenen Identitäten

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

- Die Bedingung der dynamischen Rolle trifft nicht zu.
Das kann beispielsweise auftreten, wenn die Bedingung der dynamischen Rolle geändert wurde, nachdem die Identität in die Ausschlussliste eingetragen wurde.
- ODER -
- Die ausgeschlossene Identität ist auch über einen anderen Weg an die Rolle zugewiesen.
Beispielsweise per Vererbung oder durch Direktzuweisung.

Prüfen Sie diese Einträge und korrigieren Sie die Zuweisungen.

Um widersprüchliche Einträge in der Ausschlussliste für Geschäftsrollen zu prüfen

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

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

Ausführliche Informationen zum Bearbeiten der Ausschlussliste von dynamischen Rollen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- [Dynamische Rollen für Geschäftsrollen erstellen](#) auf Seite 59

Zertifizierung von Geschäftsrollen

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

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

Um den Zertifizierungsstatus einer Geschäftsrolle manuell zu ändern

1. Bearbeiten Sie im Manager die Stammdaten der Geschäftsrolle.
2. Wählen Sie im Eingabefeld **Zertifizierungsstatus** den gewünschten Wert.
3. Speichern Sie die Änderungen.

Um den Zertifizierungsstatus von Geschäftsrollen durch Attestierungen zu ändern

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

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

Für Geschäftsrollen, die mit dem Werkzeug Analyzer angelegt wurden, wird die Attestierung und Zertifizierung automatisch gestartet, wenn der Konfigurationsparameter **QER | Attestation | OrgApproval** aktiviert ist.

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

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

Detaillierte Informationen zum Thema

- [Geschäftsrollen erstellen und bearbeiten](#) auf Seite 43
- [Allgemeine Stammdaten für Geschäftsrollen](#) auf Seite 44
- [Änderungen aus der Analyse übernehmen](#) auf Seite 76

Berichte über Geschäftsrollen

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 17: Berichte über Geschäftsrollen

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Rollen, in denen die Identitäten 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 im Manager in der Kategorie Mein One Identity Manager .

Verwandte Themen

- [Analyse von Rollenmitgliedschaften und Zuweisungen an Identitäten](#) auf Seite 52

Role Mining im One Identity Manager

Die Gestaltung von Geschäftsrollen kann auf zwei Wegen erfolgen:

- Rollenmodellierung wie unter [Geschäftsrollen verwalten](#) auf Seite 6 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 Identitäten
- eine manuelle Analyse bestimmter Identitätengruppen 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.

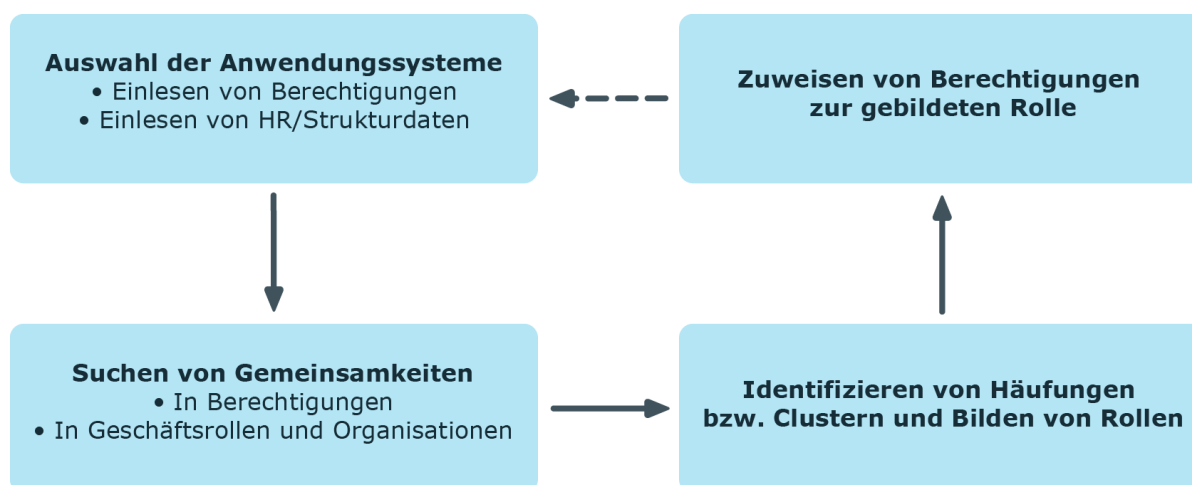
Clusteranalyse als Grundlage des Role Mining

Grundlage des Role Mining ist immer eine Clusteranalyse, bei der der Analytiker mit Hilfe eines mathematischen Algorithmus versucht, einzelne Cluster, also Identitäten 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 Rollenstrukturen dann Berechtigungen zugewiesen werden. Zuletzt können Rollenstrukturen frei definiert und die Zuordnung von Berechtigungen und Identitäten 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, HCL Domino 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 des Analyzers

Tabelle 18: Bedeutung der Einträge in der Menüleiste

Menü	Menüeintrag	Bedeutung	Tastenkombination
Datenbank	Neue Verbindung	Es wird eine Datenbankverbindung hergestellt.	Strg + Umschalt + N
	Übertragung in Datenbank	Die geänderten Zuordnungen werden in die verbundene One Identity Manager-Datenbank übertragen.	Strg + Umschalt + S
	Einstellungen	Es können allgemeine Programmeinstellungen konfiguriert werden.	
	Beenden	Das Programm wird beendet.	Alt + F4
Analyse	Vorherige Zuweisung	Es wird zur vorherigen Zuweisung der Identität/Berechtigung gesprungen.	Strg + U
	Nächste Zuweisung	Es wird zur nächsten Zuweisung der Identität/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.	

Programmeinstellungen des Analyzers

Um im Analyzer die Programmeinstellungen zu ändern

1. Wählen Sie im Analyzer den Menüeintrag **Datenbank > Einstellungen**.
2. Passen Sie die folgenden Einstellungen an.
 - **Allgemeine Sprache:** Sprache für die Formatierung von Daten wie beispielsweise Datumsformate, Zeitformate oder Zahlenformate.
 - **Andere Sprache der Benutzeroberfläche:** Sprache für die Benutzeroberfläche. Bei der ersten Anmeldung am Programm wird die Systemsprache zur Anzeige der Benutzeroberfläche verwendet. Die Änderung der Sprache wird mit dem Neustart des Programms wirksam. Die Sprache wird global für alle Programme des One Identity Manager festgelegt, somit muss die Spracheinstellung nicht in jedem Programm erneut vorgenommen werden.
 - **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
3. Übernehmen Sie die Einstellungen mit **OK**.

Durchführen einer Analyse im Analyzer

Mit dem Analyzer führen Sie folgende Schritte aus:

1. Legen Sie das Analyseverfahren fest.
 - **Analysedaten mit dem Assistenten wählen:** Die Ausgangsdaten werden mit einem Assistenten zusammengestellt.
 - **Active Directory Berechtigungen der Identitäten:** Es werden die Berechtigungen aller Identitäten mit Active Directory Gruppenmitgliedschaften

analysiert.

HINWEIS: Die Analysemethode steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

- **Active Directory Berechtigungen und Abteilungen der Identitäten:** Es werden die Berechtigungen aller Identitäten mit Active Directory Gruppenmitgliedschaften analysiert. Zusätzlich werden Abteilungen mit Active Directory Gruppen in die Analyse einbezogen.

HINWEIS: Die Analysemethode steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

- **LDAP Berechtigungen der Identitäten:** Es werden die Berechtigungen aller Identitäten mit LDAP Gruppenmitgliedschaften analysiert.

HINWEIS: Die Analysemethode steht zur Verfügung, wenn das LDAP Modul vorhanden ist.

2. Prüfen Sie die Analyseergebnisse.
3. Erstellen Sie bei Bedarf neue Geschäftsrollen und ordnen Sie die Identitäten zu. Übernehmen Sie die vorgeschlagenen Änderungen in die One Identity Manager-Datenbank.

Detaillierte Informationen zum Thema

- [Analysedaten mit dem Assistenten auswählen](#) auf Seite 70
- [Vordefinierte Analysen ausführen](#) auf Seite 73
- [Auswertung der Analyse](#) auf Seite 74
- [Änderungen aus der Analyse übernehmen](#) auf Seite 76

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 Identitäten 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 mit dem Assistenten auszuwählen

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Verwalten** den Eintrag **Geschäftsrollen analysieren**. Das Programm Analyzer wird gestartet.




3. Auf der Startseite des Analyzers wählen Sie das Analyseverfahren **Analysedaten mit Assistenten wählen** und klicken Sie **Start**.

Der Assistent wird gestartet.

4. Auf der Startseite legen Sie die Identitäten fest, die analysiert werden sollen. Wählen Sie eines der folgenden Auswahlverfahren und klicken Sie **Weiter**.

- **Strukturen:** Die Auswahl der Identitäten erfolgt über die im One Identity Manager enthalten Organisationen und Geschäftsrollen.
 1. Wählen Sie in der Liste **Strukturen** die Organisation oder Geschäftsrolle zur Analyse aus.
 2. In der Liste **Identitäten** werden die Identitäten angezeigt, die der Struktur zugeordnet sind. Über die Symbole im rechten Bereich der Identitätenliste können Sie die angezeigten Identitäten weiter filtern.

Tabelle 19: Symbole zum Filtern der Identitäten

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

- **Filterassistent:** Legen Sie die Bedingung fest, anhand der die Identitäten 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.

Ausführliche 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 Identitäten der One Identity Manager-Datenbank angezeigt. Über **Shift + Auswahl** oder **Strg + Auswahl** wählen Sie mehrere Identitäten zur Analyse aus.
 - **Assistentenvorlage laden:** Laden Sie eine vorhandene Konfiguration. Wählen Sie die Vorlagedatei und klicken Sie **Öffnen**.
5. Auf der Seite **Benutzerkonten wählen** wählen Sie das Zielsystem, dessen Benutzerkonten und Berechtigungen in die Analyse einbezogen werden. Über **Strg + Auswahl** können Sie mehrere Zielsystem auswählen.
 6. Auf der Seite **Analyseverfahren wählen** legen Sie das Analyseverfahren fest. Zur Auswahl stehen folgende Verfahren.

Tabelle 20: Analyseverfahren

Analyseverfahren	Beschreibung
Einfache Clusteranalyse/Komplexe Clusteranalyse	Die Berechtigungen werden mittels Clusteranalyseverfahren zu neuen Geschäftsrollen gruppiert und die Identitäten 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 Identitäten 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 Identitäten analysiert. Geschäftsrollen werden frei definiert und die Zuordnung von Berechtigungen und Identitäten an Hand der vorhandenen Berechtigungen manuell bewertet.

7. Auf der letzten Seite starten Sie die Analyse.
 - a. (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 an und klicken Sie **Speichern**.
 - b. Auf der letzten Seite klicken Sie **Fertig**, um die Analyse zu starten.
Die Analyseinformationen werden geladen und die Analyse gestartet.
Anschließend werden im Analyzer die Analyseergebnisse dargestellt.
8. Prüfen Sie die Analyseergebnisse.
9. Erstellen Sie bei Bedarf neue Geschäftsrollen und ordnen Sie die Identitäten zu.
Übernehmen Sie die vorgeschlagenen Änderungen in die One Identity Manager-Datenbank.

Verwandte Themen

- [Auswertung der Analyse](#) auf Seite 74
- [Änderungen aus der Analyse übernehmen](#) auf Seite 76

Vordefinierte Analysen ausführen

Es werden folgende vordefinierte Analysen zur Verfügung gestellt:

- **Active Directory Berechtigungen der Identitäten:** Es werden die Berechtigungen aller Identitäten mit Active Directory Gruppenmitgliedschaften analysiert.
HINWEIS: Die Analysemethode steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.
- **Active Directory Berechtigungen und Abteilungen der Identitäten:** Es werden die Berechtigungen aller Identitäten mit Active Directory Gruppenmitgliedschaften analysiert. Zusätzlich werden Abteilungen mit Active Directory Gruppen in die Analyse einbezogen.
HINWEIS: Die Analysemethode steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.
- **LDAP Berechtigungen der Identitäten:** Es werden die Berechtigungen aller Identitäten mit LDAP Gruppenmitgliedschaften analysiert.
HINWEIS: Die Analysemethode steht zur Verfügung, wenn das LDAP Modul vorhanden ist.

Um eine vordefinierte Analyse zu starten

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Verwalten** den Eintrag **Geschäftsrollen analysieren**. Das Programm Analyzer wird gestartet.
3. Auf der Startseite des Analyzers wählen Sie das vordefinierte Analyseverfahren und 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. Anschließend werden im Analyzer die Analyseergebnisse dargestellt.
HINWEIS: Wenn Sie die Programmeinstellung **Informationsfenster zur Datenanalyse am Ende automatisch schließen** deaktiviert haben, werden Informationen zur Analyse im Fenster **Clusteranalyse** angezeigt. Über **Erweitern** sehen Sie detaillierte Informationen. Über **Fertig** schließen Sie das Informationsfenster.
4. Prüfen Sie die Analyseergebnisse.

- Erstellen Sie bei Bedarf neue Geschäftsrollen und ordnen Sie die Identitäten zu. Übernehmen Sie die vorgeschlagenen Änderungen in die One Identity Manager-Datenbank.

Verwandte Themen

- [Auswertung der Analyse](#) auf Seite 74

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 Identitäten und Berechtigungen einer Geschäftsrolle auch direkt bearbeiten. Mit dem Analyser können Sie neue Geschäftsrollen erstellen und Identitäten direkt zuordnen. Das Hinzufügen oder das Verschieben von Identitäten in eine bestimmte Geschäftsrolle lässt sich damit einfach umsetzen.

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

Abbildung 15: Darstellung der Analyseergebnisse

The screenshot displays the One Identity Manager interface with the following components:

- Clusteranalyse (1):** A tree view showing clusters. The cluster 'Mücke, Martina' is selected and highlighted in blue.
- Personen (1):** A list of users with a similarity score bar. 'Mücke, Martina' is at the top, and 'Britt, Tanja' is highlighted with a red '2'.
- Berechtigungen (1 + 1):** A list of permissions, including 'AD Berechtigungen', 'Verteiler', 'Account Operators', 'Accountants', 'Accounting', 'Administration', 'Administratoren DEP', and 'Administrators'.
- Mitgliedschaften:** A table showing user assignments to roles. A row for 'Mücke, Martina' and 'Rittersgrün, Dr. Rüdiger von' is highlighted with a red '3'. The columns are 'Ähnlichkeit', 'AD Berechtigungen...', 'Domain Users', and 'Verteiler'.

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 Identität. 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 Identitäten 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 Identitäten oder Berechtigungen entspricht 100% und wird mit maximalen Balken dargestellt.

Tabelle 21: Bedeutung der Einträge im Kontextmenü im Bereich 1

Eintrag im Kontextmenü	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.
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 Identitäten (oben) und Berechtigungen (unten) aufgelistet. Für Identitäten 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 Identitäten in den analysierten Zielsystemen angezeigt. Abhängig von den Programmeinstellungen wird zusätzlich eine Wichtung der Berechtigungen angezeigt.

Tabelle 22: Bedeutung der Einträge im Kontextmenü im Bereich (2)

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

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

Um Mitgliedschaften von Identitäten zu vergleichen

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

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


Änderungen aus der Analyse übernehmen

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

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

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

Verwenden Sie dazu die Kontextmenüeinträge **Einfügen** oder **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. Auf der Seite **Speicheroptionen** legen Sie folgende Einstellungen fest:
 - a. **Rollenklasse**: Wählen Sie 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.
 - b. Wählen Sie die Speicheroptionen.
 - **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 Identitäten** an den Geschäftsrollen. Verwenden Sie dazu das Programm Manager.
 - **Direkte Zuordnungen entfernen**: Direkte Zuordnungen von Berechtigungen zu den Benutzerkonten der Identitäten werden entfernt.
VORSICHT: Setzen Sie diese Option nur, wenn Sie sicher gestellt haben, dass die Berechtigungen über Geschäftsrollen an die Identitäten 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.
4. Klicken Sie **Fertig**, um die Daten zu übernehmen.

Verwandte Themen

- [Zertifizierung von Geschäftsrollen](#) auf Seite 63

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

A

- Analyzer 68
 - Analysedaten 70
 - Analyseergebnis 74
 - Änderungen speichern 76
 - Assistent 70
 - Programmeinstellungen 69
 - Vordefinierte Analysen 73
- Anwendungsrolle
 - Administratoren 7
 - Attestierer 7, 41
 - Genehmiger 7, 42
 - Genehmiger (IT) 7, 42
 - Zusätzliche Manager 7
- Arbeitsplatz
 - keine Vererbung 29-30
- Ausschlussliste (dynamische Rolle)
 - fehlerhafte Einträge 62

B

- Benutzerkonto
 - Bildungsregeln ausführen 58
- Bildungsregel
 - IT Betriebsdaten ändern 58

D

- Delegierung 44
- Dynamische Rolle
 - Ausschlussliste prüfen 62
 - Identitäten ausschließen 62

G

- Gerät
 - keine Vererbung 29-30
- Geschäftsrolle
 - Attestierer 43
 - Berichte 64
 - einrichten 43
 - keine Vererbung 29
 - Lizenzknoten 43
 - Mitgliedschaft delegierbar 44
 - Unternehmensressourcen zuweisen 22
 - widersprechende Rollen 31
 - Zertifizierungsstatus 63
 - Zusatzeigenschaft zuweisen 61
 - zuweisen 13
- Geschäftsrollenstruktur 43

I

- Identität
 - keine Vererbung 29-30
- IT Betriebsdaten
 - ändern 58

R

- Risikobewertung
 - Unternehmensbereich 39
- Role Mining 66
 - Analysedaten 70

- Analyseergebnis 74
- Analyzer 68
- Clusteranalyse 67
- Rollen
 - Grundlagen 8
 - keine Vererbung 29
 - Vererbung
 - Bottom-Up 9
 - Top-Down 9
- Rollenklasse 35
 - Delegierung 44
 - Rollentyp 36, 39
 - Vererbungsrichtung 28
 - Zuweisung erlauben 27
- Rollentyp 37-38
 - Rollenklasse 36, 39
 - zuweisen 36, 39

U

- Unternehmensbereich 39
- Unternehmensressourcen
 - zuweisen 13

V

- Vererbung
 - blockieren 29
 - Bottom-Up 9
 - einschränken 29-30
 - Top-Down 9
 - unterbrechen 11, 29
- Vererbungsausschluss 31
 - für Geschäftsrollen definieren 60
- Vererbungsrichtung 28

W

- Widersprechende Geschäftsrolle 60

Z

- Zertifizierung 63
- Zertifizierungsstatus 63
- Zuweisung
 - direkt 14
 - dynamische Rolle 16
 - erlauben 27
 - indirekt 14
 - IT Shop 17
 - primär 15
 - Konfiguration 15
 - sekundär 14
 - über IT Shop Bestellung 17
 - Unternehmensressourcen 22
- Zuweisungsressource
 - für eine Geschäftsrolle 62