

One Identity Manager 9.0

Administrationshandbuch für Systemrollen

Copyright 2022 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

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

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

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

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

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

Patente

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

Marken

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

Legende

WARNUNG: Das Symbol WARNUNG weist auf 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 Systemrollen
Aktualisiert - 01. August 2022, 16:21 Uhr
Version - 9.0

Inhalt

Verwalten von Systemrollen **5**
One Identity Manager Benutzer für die Verwaltung von Systemrollen 6

Grundlagen zur Berechnung der Vererbung von Systemrollen **8**
Details zur Vererbung von Systemrollen 9
Wirksamkeit von Systemrollen 10
Deaktivierte Systemrollen 12

Systemrollen erstellen und bearbeiten **13**
Allgemeine Stammdaten für Systemrollen 14
Systemrollentypen erstellen und bearbeiten 16
Unternehmensressourcen an Systemrollen zuweisen 16
Systemrollen an Personen und Arbeitsplätze zuweisen 18
Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen 20
Systemrollen an Geschäftsrollen zuweisen 21
Systemrollen in den IT Shop aufnehmen 21
Systemrollen direkt an Personen zuweisen 23
Systemrollen direkt an Arbeitsplätze zuweisen 23
Systemrollen in Systemrollen aufnehmen 24
Systemrollen zuweisen 25
Systemrollen ausschließen 26
Zusatzeigenschaften an Systemrollen zuweisen 27
Überblick über Systemrollen anzeigen 27

Anhang: Konfigurationsparameter für Systemrollen **28**

Anhang: Beispiele zur Vererbung von Systemrollen **30**
Beispiel für eine Systemrollenhierarchie 30
Beispiele für Vererbungswege für Systemrollen 31
Wirkung von Ausschlussdefinitionen für Systemrollen 33
Besonderheiten bei der Vererbung von Systemrollen über hierarchische Rollen 35

Über uns **38**
Kontaktieren Sie uns 38
Technische Supportressourcen 38

Index **39**

Verwalten von Systemrollen

Systemrollen vereinfachen die Zuweisung von häufig benötigten Unternehmensressourcen beziehungsweise Unternehmensressourcen, die immer gemeinsam zugewiesen werden müssen. Beispielsweise sollen neue Mitarbeiter im Bereich Finanzen eines Unternehmens standardmäßig mit bestimmten Systemberechtigungen für eine Active Directory-Umgebung und ein SAP R/3 System und mit bestimmter Software ausgestattet werden. Um zahlreiche Einzelzuweisungen zu vermeiden, fassen Sie diese Unternehmensressourcen zu einem Paket zusammen und weisen dieses den neuen Mitarbeitern zu. Solche Pakete werden im One Identity Manager als Systemrollen bezeichnet.

Mit Systemrollen können Sie beliebige Unternehmensressourcen zusammenzufassen. Diese Systemrollen können Sie an Personen, Arbeitsplätze oder Rollen zuweisen oder über den IT Shop bestellen. Unternehmensressourcen, die den Systemrollen zugewiesen sind, werden an die Personen und Arbeitsplätze vererbt. Indem Sie Systemrollen an Systemrollen zuweisen, können Sie Systemrollen strukturieren.

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

Die One Identity Manager Bestandteile für Verwaltung von Systemrollen sind verfügbar, wenn der Konfigurationsparameter **QER | ESet** 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*.

Detaillierte Informationen zum Thema

- One Identity Manager Benutzer für die Verwaltung von Systemrollen auf Seite 6
- Grundlagen zur Berechnung der Vererbung von Systemrollen auf Seite 8
- Systemrollen erstellen und bearbeiten auf Seite 13

- Konfigurationsparameter für Systemrollen auf Seite 28
- Beispiele zur Vererbung von Systemrollen auf Seite 30

One Identity Manager Benutzer für die Verwaltung von Systemrollen

In die Verwaltung von Systemrollen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Verantwortliche für die einzelnen Unternehmensressourcen	Die Benutzer werden über die verschiedenen Anwendungsrollen für Administratoren und Verantwortliche definiert. Benutzer mit diesen Anwendungsrollen: • Erstellen und Bearbeiten die Systemrollen. • Weisen Systemrollen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zu. • Weisen Systemrollen an Personen zu. • Weisen Systemrollen an Arbeitsplätze zu.
Produkteigner für den IT Shop	Die Produkteigner müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über Bestellungen. • Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind. Es kann die Standard-Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | Systemrollen** genutzt werden.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen.

Benutzer	Aufgaben
	• 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.

Grundlagen zur Berechnung der Vererbung von Systemrollen

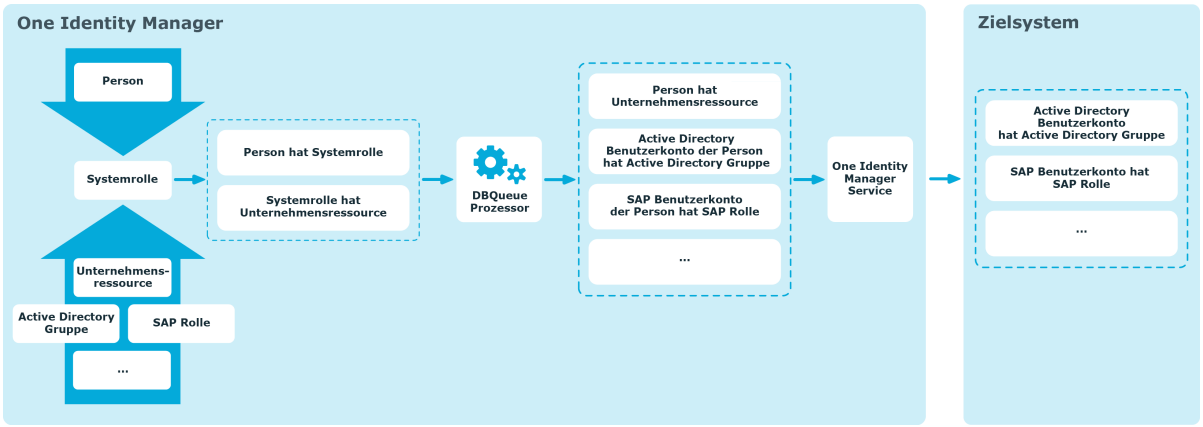
An Systemrollen können beliebige Unternehmensressourcen sowie andere Systemrollen zugewiesen werden. Durch die Zuweisung von Systemrollen an andere Systemrollen können die Systemrollen hierarchisch strukturiert werden. Systemrollen können auf folgenden Wegen an Personen und Arbeitsplätze zugewiesen werden:

- Direktzuweisung
- IT Shop-Bestellung
- Vererbung über hierarchische Rollen
- Vererbung über dynamische Rollen

Eine Person (ein Arbeitsplatz, eine hierarchische Rolle) erbt alle Unternehmensressourcen, die der Systemrolle zugewiesen sind. Untergeordnete Systemrollen werden dabei aufgelöst. Voraussetzung ist, dass die einzelne Unternehmensressource tatsächlich vererbt werden kann.

HINWEIS: Damit eine Zielsystemberechtigung vererbt werden kann, muss die Person ein Benutzerkonto in diesem Zielsystem besitzen.

Abbildung 1: Vererbung von Unternehmensressourcen über Systemrollen



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.

Detaillierte Informationen zum Thema

- Details zur Vererbung von Systemrollen auf Seite 9
- Wirksamkeit von Systemrollen auf Seite 10
- Deaktivierte Systemrollen auf Seite 12
- Beispiel für eine Systemrollenhierarchie auf Seite 30

Details zur Vererbung von Systemrollen

Die Zuweisungen von Unternehmensressourcen zu Systemrollen werden in der Tabelle `ESetHasEntitlement` abgebildet.

Über die Beziehung `UID_ESet - Entitlement` wird die Systemrollenhierarchie abgebildet. Die Systemrollenhierarchie ist in der Tabelle `ESetCollection` abgelegt. Dabei werden alle Systemrollen aufgezählt, von denen die angegebene Systemrolle erbt. Jede Systemrolle erbt auch von sich selbst.

In der Tabelle `ESetCollection` gilt folgende Beziehung:

- `UID_ESet` ist die Systemrolle, die erbt.
- `UID_ESetChild` ist die Systemrolle, die vererbt.

Die Tabelle `ESetHasEntitlement` enthält die Direktzuweisungen (`XOrigin = 1`) und alle Systemrollen, die untergeordneten Systemrollen zugewiesen sind (`XOrigin = 2`). Die Unternehmensressourcen, die einer untergeordneten Systemrolle zugewiesenen sind, werden erst bei der Vererbungsberechnung für Personen, Arbeitsplätze und hierarchische Rollen aufgelöst.

Die Zuweisungen von Systemrollen an hierarchische Rollen werden in der Tabelle `BaseTreeHasESet` abgebildet.

Eine Person kann Systemrollen direkt erhalten. Weiterhin erbt eine Person alle (auch vererbte) Systemrollen aller hierarchischen Rollen, in denen sie Mitglied ist (Tabelle `PersonInBaseTree`) sowie die Systemrollen aller hierarchischen Rollen, die über Fremdschlüssel-Beziehungen referenziert werden (Tabelle `Person`, Spalte `UID_<BaseTree>`). Die direkten und indirekten Zuweisungen der Systemrollen an Personen werden in der Tabelle `PersonHasESet` abgebildet. Dieses Verhalten gilt analog für die Zuweisung von Systemrollen an Arbeitsplätze.

Detaillierte Informationen zum Thema

- Beispiele für Vererbungswege für Systemrollen auf Seite 31

Wirksamkeit von Systemrollen

Durch die Zuweisung von Systemrollen an Personen, Arbeitsplätze oder hierarchische Rollen kann es vorkommen, dass eine Person verschiedene Unternehmensressourcen erhält, die in dieser Kombination nicht zugewiesen sein dürfen. Um das zu verhindern, geben Sie die sich ausschließenden Systemrollen bekannt. Dabei legen Sie für zwei Systemrollen fest, welche der beiden Systemrollen wirksam sein soll, wenn beide zugewiesen sind. Über die unwirksame Systemrolle werden keine Unternehmensressourcen vererbt.

Voraussetzung

- Der Konfigurationsparameter **QER | Structures | Inherite | ESetExclusion** ist aktiviert.

  Aktivieren Sie im Designer 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*.

Die Zuweisung von Personen, Arbeitsplätzen und Unternehmensressourcen an eine ausgeschlossene Systemrolle ist jederzeit direkt, indirekt oder per IT Shop-Bestellung möglich. Anschließend ermittelt der One Identity Manager, ob diese Zuweisung wirksam ist und die Unternehmensressourcen vererbt werden.

> HINWEIS:
>
> - Ein wechselseitiger Ausschluss zweier Systemrollen kann nicht definiert werden. Das heißt, die Festlegung "Systemrolle A schließt Systemrolle B aus" `UND` "Systemrolle B schließt Systemrolle A aus" ist nicht zulässig.
> - Für eine Systemrolle muss jede auszuschließende Systemrolle einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `PersonHasESet`, `BaseTreeHasESet` und `WorkdeskHasESet` über die Spalte `XIsInEffect` abgebildet.

> HINWEIS: Wenn eine Unternehmensressource, die einer ausgeschlossenen Systemrolle zugewiesen ist, selbst direkt oder indirekt an eine Person oder einen Arbeitsplatz zugewiesen ist, dann wirkt die Ausschlussdefinition auf diese Unternehmensressource nicht. Die Ausschlussdefinition wirkt nur auf die Systemrollen.

Beispiel: Wirksamkeit von Systemrollen

- Die Systemrolle "Marketing" enthält alle Software-Anwendungen und Berechtigungen zum Auslösen von Bestellungen.
- Die Systemrolle "Finanzen" enthält alle Software-Anwendungen und Berechtigungen zum Anweisen von Zahlungen.
- Die Systemrolle "Controlling" enthält alle Software-Anwendungen und Berechtigungen zum Prüfen von Rechnungen.

Clara Harris wird die Systemrolle "Marketing" direkt zugewiesen. Die Systemrolle "Finanzen" und die Systemrolle "Controlling" erhält sie über eine IT Shop-Bestellung. Ohne Ausschlussdefinition erhält Clara Harris alle Systemrollen und die damit verbundenen Berechtigungen.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person, die Rechnungen zur Zahlung anweisen darf, auch Bestellungen auslösen kann. Das heißt, die Systemrollen "Finanzen" und "Marketing" schließen sich aus. Eine Person, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Systemrollen "Finanzen" und "Controlling" schließen sich aus.

Tabelle 2: Festlegen der ausgeschlossenen Systemrollen (Tabelle `ESetExcludesESet`)

Wirksame Systemrolle	Ausgeschlossene Systemrolle
Finanzen	Marketing
Controlling	Finanzen

Tabelle 3: Wirksame Zuweisungen

Person	Zugewiesene Systemrolle	Wirksame Systemrolle
Ben King	Marketing	Marketing
Jan Bloggs	Marketing, Finanzen	Finanzen
Clara Harris	Marketing, Finanzen, Controlling	Controlling
Jenny Basset	Marketing, Controlling	Marketing, Controlling

Für Clara Harris ist nur die Zuweisung der Systemrolle "Controlling" wirksam. Wird ihr die Systemrolle "Controlling" zu einem späteren Zeitpunkt entzogen, dann wird die Zuweisung der Systemrolle "Finanzen" wieder wirksam.

Für Jenny Basset bleiben die Zuweisungen der Systemrollen "Marketing" und "Controlling" erhalten, da zwischen beiden Systemrollen kein Ausschluss definiert wurde. Das heißt, die Person ist berechtigt Bestellungen auszulösen und Rechnungen

zu prüfen. Soll auch das verhindert werden, definieren Sie einen weiteren Ausschluss für die Systemrolle "Controlling".

Tabelle 4: Ausgeschlossene Systemrollen und wirksame Zuweisungen

Person	Zugewiesene Systemrolle	Ausgeschlossene Systemrolle (`UID_ESetExcluded`)	Wirksame Systemrolle
Jenny Basset	Marketing		Controlling
	Controlling	Finanzen	
		Marketing	

Detaillierte Informationen zum Thema

- Wirkung von Ausschlussdefinitionen für Systemrollen auf Seite 33
- Besonderheiten bei der Vererbung von Systemrollen über hierarchische Rollen auf Seite 35
- Systemrollen ausschließen auf Seite 26

Deaktivierte Systemrollen

Systemrollen können deaktiviert werden, beispielsweise um zeitweilig zu verhindern, dass die enthaltenen Unternehmensressourcen an Personen und Arbeitsplätze vererbt werden. Wird eine Systemrolle deaktiviert, berechnet der DBQueue Prozessor die Vererbung der enthaltenen Unternehmensressourcen neu. Bestehende Zuweisungen an Personen und Arbeitsplätze werden entfernt. Die deaktivierte Systemrolle bleibt zugewiesen; die Zuweisung ist aber nicht mehr wirksam (`PersonHasESet.XIsInEffect = 0`). Sobald die Systemrolle wieder aktiviert wird, wird die Vererbung der Unternehmensressourcen erneut berechnet. Die enthaltenen Unternehmensressourcen werden an Personen und Arbeitsplätze zugewiesen.

Eine deaktivierte Systemrolle kann nicht im Web Portal bestellt werden. Eine deaktivierte Systemrolle kann aber direkt an Personen, Arbeitsplätze, hierarchische und dynamische Rollen und an IT Shop Regale zugewiesen werden.

Verwandte Themen

- Allgemeine Stammdaten für Systemrollen auf Seite 14

Systemrollen erstellen und bearbeiten

Um eine Systemrolle zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste eine Systemrolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Systemrollen auf Seite 14
- Systemrollentypen erstellen und bearbeiten auf Seite 16
- Unternehmensressourcen an Systemrollen zuweisen auf Seite 16
- Systemrollen an Personen und Arbeitsplätze zuweisen auf Seite 18
- Systemrollen ausschließen auf Seite 26
- Zusatzeigenschaften an Systemrollen zuweisen auf Seite 27
- Überblick über Systemrollen anzeigen auf Seite 27
- Konfigurationsparameter für Systemrollen auf Seite 28

Allgemeine Stammdaten für Systemrollen

Für Systemrollen erfassen Sie folgende Stammdaten.

Tabelle 5: Stammdaten einer Systemrolle

Eigenschaft	Beschreibung
Anzeigename	Bezeichnung unter der die Systemrolle in den Werkzeugen des One Identity Manager angezeigt werden soll.
Systemrolle	Eindeutige Bezeichnung für die Systemrolle.
Interner Produktname	Zusätzliche interne Bezeichnung für die Systemrolle.
Systemrollentyp	Gibt an, welcher Art Unternehmensressourcen in der Systemrolle zusammengefasst werden.
Leistungsposition	Um eine Systemrolle innerhalb des IT Shops zu verwenden, weisen Sie ihr eine Leistungsposition zu oder legen Sie eine neue Leistungsposition an. Ausführliche Informationen über Leistungspositionen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Verantwortlicher der Systemrolle	Verantwortlicher für die Systemrolle. Ordnen Sie eine beliebige Person zu. Diese Person kann die Stammdaten der Systemrolle bearbeiten. Sie kann als Attestierer für die Eigenschaften der Systemrolle ermittelt werden. Wenn die Systemrolle im IT Shop bestellt werden kann, wird der Verantwortliche automatisch Mitglied in der Anwendungsrolle für Produkteigner, die der Leistungsposition zugeordnet ist.
Freigabedatum	Legen Sie einen Zeitpunkt fest, an dem die Systemrolle aktiviert werden soll. Liegt das Freigabedatum in der Zukunft, wird die Systemrolle als deaktivierte Systemrolle behandelt. Ist das Freigabedatum erreicht wird die Systemrolle aktiviert. Unternehmensressourcen, die der Systemrolle zugewiesen sind, werden an Personen vererbt. Ist das Freigabedatum überschritten oder ist kein Datum eingetragen, wird die Systemrolle als aktivierte Systemrolle behandelt. Die Vererbung der Unternehmensressourcen kann in diesen Fällen über die Option **Deaktiviert** gesteuert werden. HINWEIS: Konfigurieren und aktivieren Sie im Designer den Zeitplan **Systemrollen freigeben**, um das Freigabedatum zu überprüfen. Ausführliche Informationen zu Zeitplänen finden Sie im *One Identity Manager Administrationshandbuch für betriebs-*

Eigenschaft	Beschreibung
	unterstützende Aufgaben.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Unternehmensressourcen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Berechnung des Risikoindex finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Deaktiviert	Gibt an, ob die Unternehmensressourcen, die in der Systemrolle zusammengefasst sind, an Personen und Arbeitsplätze vererbt werden. Ist die Option aktiviert, kann die Systemrolle an Personen, Arbeitsplätze, hierarchische Rollen und IT Shop Regale zugewiesen werden. Die enthaltenen Unternehmensressourcen werden jedoch nicht vererbt. Die Systemrolle kann nicht im Web Portal bestellt werden. Ist die Option deaktiviert, werden die Unternehmensressourcen, die der Systemrolle zugewiesen sind, vererbt. Wird die Option zu einem späteren Zeitpunkt aktiviert, werden bestehende Zuweisungen entfernt.
IT Shop	Gibt an, ob die Systemrolle über den IT Shop bestellbar ist. Die Systemrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Systemrolle kann weiterhin direkt an Personen und hierarchische Rollen zugewiesen werden. Ausführliche Informationen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Verwendung im IT Shop	Gibt an, ob die Systemrolle ausschließlich über den IT Shop bestellbar ist. Die Systemrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Systemrolle an hierarchische Rollen ist nicht zulässig.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Deaktivierte Systemrollen auf Seite 12

Systemrollentypen erstellen und bearbeiten

Systemrollentypen kennzeichnen die Art der Unternehmensressourcen, die in einer Systemrolle zusammengefasst werden. Sie können beispielsweise Systemrollentypen für Systemrollen definieren, in denen verschiedene Zielsystemgruppen zusammengefasst werden sollen.

Um Systemrollentypen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Basisdaten zur Konfiguration > Systemrollentypen**.
2. Wählen Sie in der Ergebnisliste einen Systemrollentyp. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   – ODER –

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

Unternehmensressourcen an Systemrollen zuweisen

Weisen Sie der Systemrolle die Unternehmensressourcen zu, die Sie zu einem Paket zusammenfassen wollen. Wenn Sie die Systemrolle an Personen und Arbeitsplätze zuweisen, werden diese Unternehmensressourcen an die Personen und Arbeitsplätze vererbt.

HINWEIS: Unternehmensressourcen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist.

In der nachfolgenden Tabelle sind die Unternehmensressourcen aufgeführt, die Sie an Systemrollen zuweisen können.

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

Tabelle 6: Mögliche Zuweisungen von Unternehmensressourcen

Unternehmensressource	Verfügbar im Modul
Ressourcen	immer
Kontendefinitionen	Zielsystem Basismodul
Gruppen kundendefinierter Zielsysteme	Zielsystem Basismodul
Systemberechtigungen kundendefinierter Zielsysteme	Zielsystem Basismodul
Active Directory Gruppen	Active Directory Modul
SharePoint Gruppen	SharePoint Modul
SharePoint Rollen	SharePoint Modul
LDAP Gruppen	LDAP Modul
Notes Gruppen	Domino Modul
SAP Gruppen	SAP R/3 Benutzermanagement-Modul
SAP Profile	SAP R/3 Benutzermanagement-Modul
SAP Rollen	SAP R/3 Benutzermanagement-Modul
SAP Parameter	SAP R/3 Benutzermanagement-Modul
Strukturelle Profile	Modul SAP R/3 Strukturelle Profile Add-on
BI Analyseberechtigungen	Modul SAP R/3 Analyseberechtigungen Add-on
E-Business Suite Berechtigungen	Oracle E-Business Suite Modul
Abonnierbare Berichte	Modul Berichtsabonnement
Software	Modul Softwaremanagement
Azure Active Directory Gruppen	Azure Active Directory Modul
Azure Active Directory Administratorrollen	Azure Active Directory Modul
Azure Active Directory Abonnements	Azure Active Directory Modul
Unwirksame Azure Active Directory Dienstpläne	Azure Active Directory Modul
Unix Gruppen	Modul Unix-basierte Zielsysteme
Cloud Gruppen	Modul Cloud Systems Management

Unternehmensressource	Verfügbar im Modul
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 Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
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.

Verwandte Themen

- Systemrollen zuweisen auf Seite 25

Systemrollen an Personen und Arbeitsplätze zuweisen

Systemrollen können direkt oder indirekt an Personen oder Arbeitsplätze zugewiesen werden. Bei der indirekten Zuweisung werden Personen (Arbeitsplätze) und Systemrollen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Systemrollen, die einer Person (einem Arbeitsplatz) zugewiesen ist.

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

HINWEIS: Ist die Systemrolle deaktiviert oder liegt das Freigabedatum in der Zukunft, werden die Unternehmensressourcen nicht vererbt.

Voraussetzung für die indirekte Zuweisung an Personen

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

Voraussetzung für die indirekte Zuweisung an Arbeitsplätze

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

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

   - ODER -

   Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
   - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
   - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle blockiert sein oder die Vererbung an Personen nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 20
- Systemrollen an Geschäftsrollen zuweisen auf Seite 21
- Systemrollen in den IT Shop aufnehmen auf Seite 21
- Systemrollen direkt an Personen zuweisen auf Seite 23
- Systemrollen direkt an Arbeitsplätze zuweisen auf Seite 23
- Systemrollen in Systemrollen aufnehmen auf Seite 24

- Unternehmensressourcen an Systemrollen zuweisen auf Seite 16
- Details zur Vererbung von Systemrollen auf Seite 9

Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Systemrolle an Abteilungen, Kostenstellen oder Standorte zu, damit die Systemrolle über diese Organisationen an Personen und Arbeitsplätze zugewiesen wird.

Um eine Systemrolle an Abteilungen, Kostenstellen oder Standorte zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

   Um eine Zuweisung zu entfernen

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

HINWEIS: Damit die Unternehmensressourcen, die der Systemrolle zugewiesen sind, an die Abteilungen, Kostenstellen oder Standorte vererbt werden, muss an den Rollenklassen die Option **Direkte Zuweisungen erlaubt** aktiviert sein. Ausführliche Informationen zum Aktivieren diese Option finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Systemrollen an Geschäftsrollen zuweisen auf Seite 21
- Systemrollen in den IT Shop aufnehmen auf Seite 21
- Systemrollen direkt an Personen zuweisen auf Seite 23
- Systemrollen direkt an Arbeitsplätze zuweisen auf Seite 23

Systemrollen an Geschäftsrollen zuweisen

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

Weisen Sie die Systemrolle an Geschäftsrollen zu, damit die Systemrolle über diese Geschäftsrollen an Personen und Arbeitsplätze zugewiesen wird.

Um eine Systemrolle an Geschäftsrollen zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

HINWEIS: Damit die Unternehmensressourcen, die der Systemrolle zugewiesen sind, an die Geschäftsrollen vererbt werden, muss an den Rollenklassen die Option **Direkte Zuweisungen erlaubt** aktiviert sein. Ausführliche Informationen zum Aktivieren diese Option finden Sie im *One Identity Manager Administrationshandbuch für Geschäftsrollen*.

Verwandte Themen

- Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 20
- Systemrollen in den IT Shop aufnehmen auf Seite 21
- Systemrollen direkt an Personen zuweisen auf Seite 23
- Systemrollen direkt an Arbeitsplätze zuweisen auf Seite 23

Systemrollen in den IT Shop aufnehmen

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

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

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

Um eine Systemrolle in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrolle an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Systemrolle aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe**In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrolle aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Systemrolle aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

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

Verwandte Themen

- Allgemeine Stammdaten für Systemrollen auf Seite 14
- Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 20
- Systemrollen an Geschäftsrollen zuweisen auf Seite 21
- Systemrollen direkt an Personen zuweisen auf Seite 23
- Systemrollen direkt an Arbeitsplätze zuweisen auf Seite 23

Systemrollen direkt an Personen zuweisen

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

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Systemrolle direkt an Personen zuweisen. Die Personen erhalten alle Unternehmensressourcen, die der Systemrolle zugewiesen sind.

HINWEIS: Ist die Systemrolle deaktiviert oder liegt das Freigabedatum in der Zukunft, werden die Unternehmensressourcen nicht vererbt.

Um eine Systemrolle direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 20
- Systemrollen an Geschäftsrollen zuweisen auf Seite 21
- Systemrollen in den IT Shop aufnehmen auf Seite 21
- Systemrollen direkt an Arbeitsplätze zuweisen auf Seite 23

Systemrollen direkt an Arbeitsplätze zuweisen

Systemrollen können direkt oder indirekt an Arbeitsplätze zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung des Arbeitsplatzes und der Systemrollen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Systemrolle direkt an Arbeitsplätze zuweisen. Die Arbeitsplätze erhalten alle Unternehmensressourcen, die der Systemrolle zugewiesen sind.

HINWEIS: Ist die Systemrolle deaktiviert oder liegt das Freigabedatum in der Zukunft, werden die Unternehmensressourcen nicht vererbt.

Um eine Systemrolle direkt an Arbeitsplätze zuzuweisen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **An Arbeitsplätze zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Arbeitsplätze zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Arbeitsplatz und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Systemrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 20
- Systemrollen an Geschäftsrollen zuweisen auf Seite 21
- Systemrollen in den IT Shop aufnehmen auf Seite 21
- Systemrollen direkt an Personen zuweisen auf Seite 23

Systemrollen in Systemrollen aufnehmen

Mit dieser Aufgabe können Sie verschiedene Systemrollen zu einem Paket zusammenfassen. Systemrollen lassen sich damit nach verschiedenen Aspekten strukturieren.

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

Um eine Systemrolle an Systemrollen zuzuordnen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.

4. Um übergeordnete Systemrollen zuzuweisen, wählen Sie den Tabreiter **Systemrolle ist enthalten in**.
    - Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

      Um eine Zuweisung zu entfernen
        - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Um untergeordnete Systemrolle zuzuweisen, wählen Sie den Tabreiter **Systemrolle enthält**.
    - Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

      Um eine Zuweisung zu entfernen
        - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Systemrollen zuweisen

Durch die Zuweisung von Systemrollen an andere Systemrollen, werden die Systemrollen hierarchisch strukturiert. Einer Systemrolle können beliebige andere Systemrollen unter- und übergeordnet werden.

In der Vererbungsberechnung werden untergeordnete Systemrollen nicht wie zugewiesene Unternehmensressourcen behandelt. Die Zuweisung von Systemrollen an Systemrollen dient nur zum Aufbau einer Hierarchie.

Um Systemrollen hierarchisch zu strukturieren

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste eine Systemrolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Wählen Sie den Tabreiter **Systemrolle enthält**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu, die der gewählten Systemrolle untergeordnet werden sollen.

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

   Um eine Zuweisung zu entfernen
    - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
6. Wählen Sie den Tabreiter **Systemrolle ist enthalten in**.

7. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu, die der gewählten Systemrolle übergeordnet werden sollen.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

8. Speichern Sie die Änderungen.

Verwandte Themen

- Unternehmensressourcen an Systemrollen zuweisen auf Seite 16

Systemrollen ausschließen

Legen Sie für zwei Systemrollen fest, welche der beiden Systemrollen wirksam sein soll, wenn beide zugewiesen sind. Über die unwirksame Systemrolle werden keine Unternehmensressourcen vererbt.

Um Systemrollen auszuschließen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste eine Systemrolle.
3. Wählen Sie die Aufgabe **Systemrollen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu, die sich mit der gewählten Systemrolle ausschließen.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Wirksamkeit von Systemrollen auf Seite 10

Zusatzeigenschaften an Systemrollen zuweisen

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

Um Zusatzeigenschaften für eine Systemrolle festzulegen

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Überblick über Systemrollen anzeigen

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

Um einen Überblick über eine Systemrolle zu erhalten

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Systemrollen**.
2. Wählen Sie in der Ergebnisliste die Systemrolle.
3. Wählen Sie die Aufgabe **Überblick über die Systemrolle**.

Anhang A

Konfigurationsparameter für Systemrollen

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

Tabelle 7: Konfigurationsparameter für das Modul

Konfigurationsparameter	Beschreibung
QER | ESet	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für Systemrollen. Ist der Parameter aktiviert, sind die Bestandteile für Systemrollen verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | Structures | Inherite | ESetExclusion	Präprozessorrelevanter Konfigurationsparameter zur Definition der Wirksamkeit von Systemrollen. Ist der Parameter aktiviert, können sich ausschließende Systemrollen definiert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

Konfigurationsparameter	Beschreibung
QER | Structures | Inherite | NoESetSplitting	Angabe, ob die Bestandteile einer Systemrolle bereits an der hierarchischen Rolle aufgelöst werden (früheres Verhalten) oder nicht (aktuelles Verhalten). Bei Aktivierung werden die Systemrollen erst am Ziel der Vererbung in ihre einzelnen Bestandteile zerlegt. Der Konfigurationsparameter wirkt nicht auf untergeordnete Systemrollen.

Anhang B

Beispiele zur Vererbung von Systemrollen

Die folgenden Beispiele zeigen, wie die Vererbung von Unternehmensressourcen über Systemrollen funktioniert und wie sich Ausschlussdefinitionen auswirken.

Beispiel für eine Systemrollenhierarchie

Folgende Tabellen zeigen, wie Zuweisungen an Systemrollen und die Systemrollenhierarchie in der One Identity Manager-Datenbank abgebildet werden.

Tabelle 8: Systemrollen: Zuweisungen (Tabelle `ESetHasEntitlement`)

Systemrolle (`UID_ESet`)	**Zuweisung Systemrolle (`Entitlement`)**	**Herkunft (`XOrigin`)**
System role A	System role A1	1
System role A	System role A2	1
System role A	System role A11	2
System role A	System role A12	2
System role A1	System role A11	1
System role A1	System role A12	1
System role A1	System entitlement	1
System role A2	Software	1
System role A11	Active Directory group	1
System role A12	SAP role	1
System role B	Resource	1

Tabelle 9: Systemrollenhierarchie (Tabelle `ESetCollection`)

Systemrolle (`UID_ESet`)	**Untergeordnete Systemrolle (`UID_ESetChild`)**
System role A	System role A
System role A	System role A1
System role A	System role A2
System role A	System role A11
System role A	System role A12
System role A1	System role A1
System role A1	System role A11
System role A1	System role A12
System role A11	System role A11
System role A12	System role A12
System role A2	System role A2
System role B	System role B

Beispiele für Vererbungswege für Systemrollen

Abbildung 2: Vererbung einer Active Directory Gruppe über eine direkt zugewiesene Systemrolle

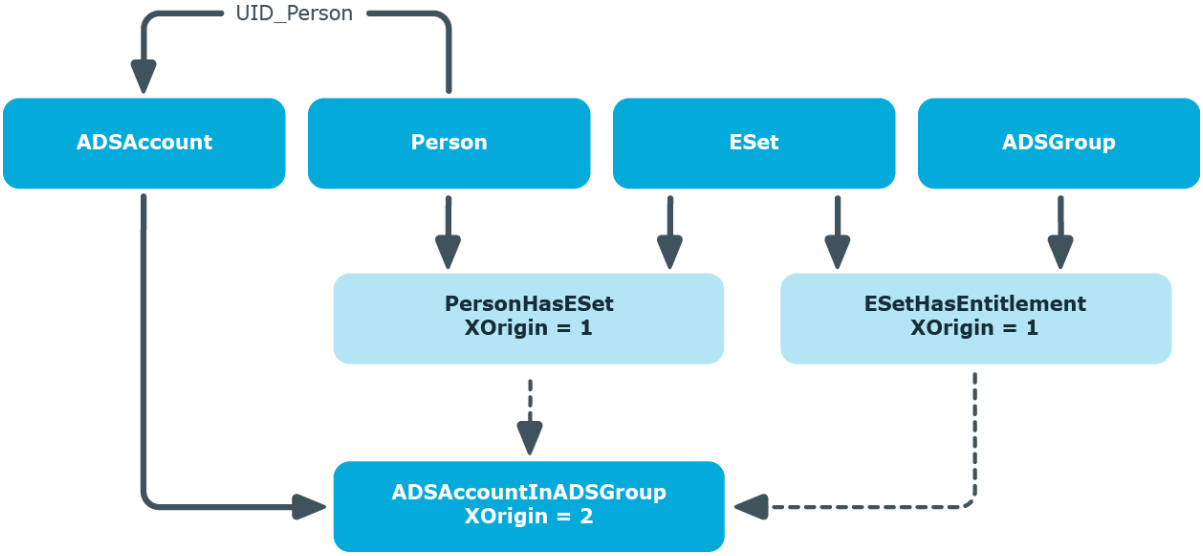


Abbildung 3: Vererbung von Software über eine IT Shop-Bestellung

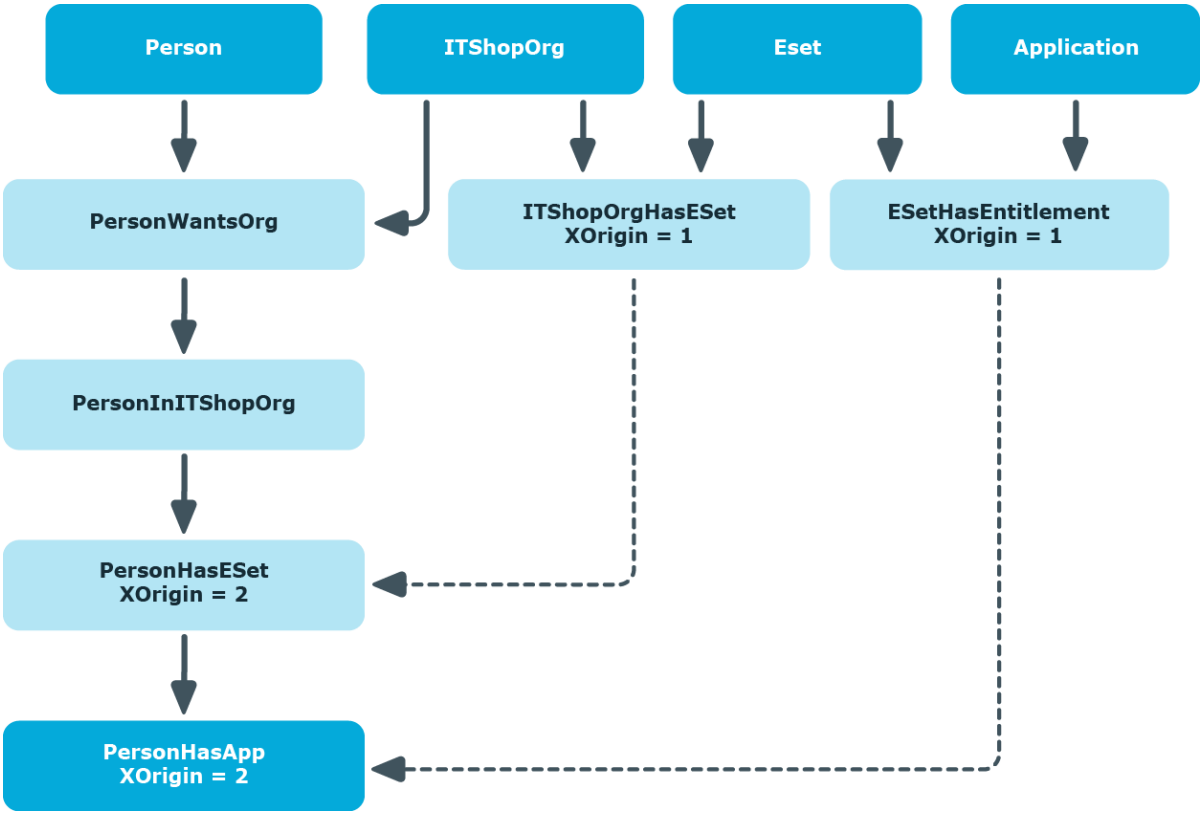
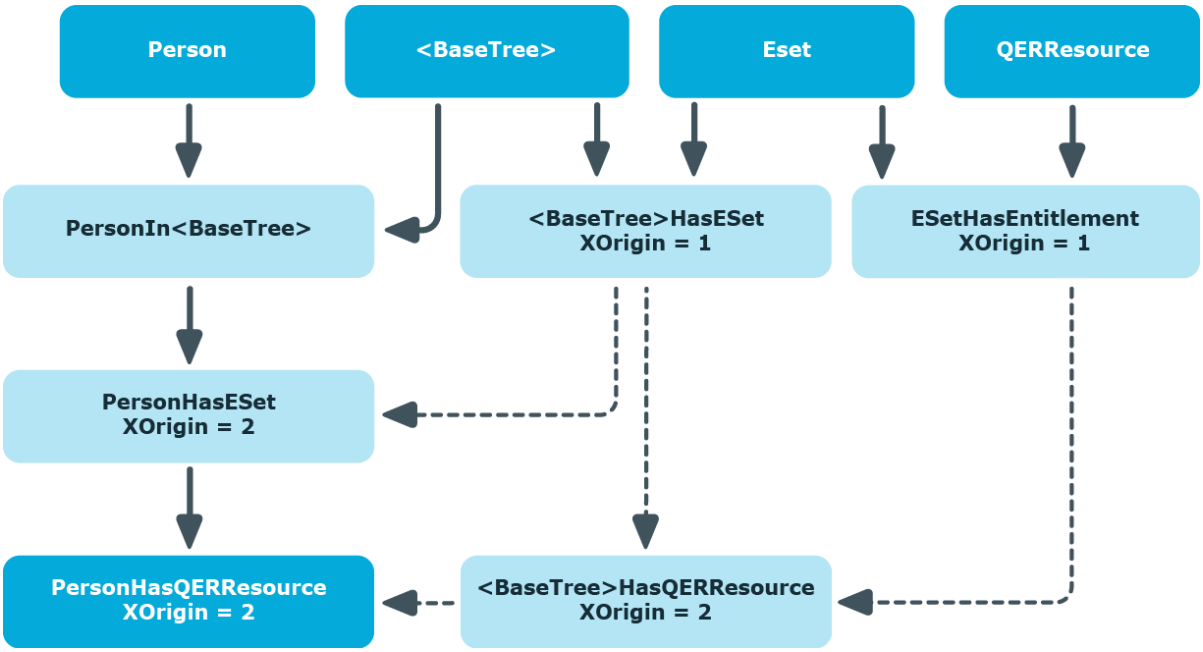


Abbildung 4: Vererbung einer Ressource über eine indirekt zugewiesene Systemrolle



Wirkung von Ausschlussdefinitionen für Systemrollen

Folgende Abbildungen zeigen, wie sich der Ausschluss einer Systemrolle in der Vererbungsberechnung auswirkt. Auch ausgeschlossene Systemrollen können an Personen zugewiesen werden. Über die Spalte `XIsInEffect` wird gekennzeichnet, ob diese Zuweisung wirksam ist. Die Zuweisung einer ausgeschlossenen Systemrolle führt zu einem Eintrag mit `XIsInEffect = 0`, wenn gleichzeitig die andere Systemrolle aus der Ausschlussdefinition zugewiesen ist.

Tabelle 10: Ausgeschlossene Systemrollen (Tabelle `ESetExcludesESet`)

Systemrolle (`UID_ESet`)	**Ausgeschlossene Systemrolle (`UID_ESetExcluded`)**
System role A12	System role A11
System role B	System role B1
System role B	System role A2

Tabelle 11: Systemrollen: Vererbung (Tabelle `ESetHasEntitlement`)

Systemrolle (`UID_ESet`)	**Zuweisung Systemrolle (`Entitlement`)**	**Zuweisung wirksam (`XIsInEffect`)**
System role A	System role A1	1
System role A	System role A2	1
System role A	System role A11	0
System role A	System role A12	1
System role A1	System role A11	0
System role A1	System role A12	1
System role A2	Software	1
System role A11	Active Directory group	1
System role A12	SAP role	1
System role B	Resource R1	1
System role B1	Resource R2	1

Abbildung 5: Vererbung über direkt zugewiesene Systemrollen

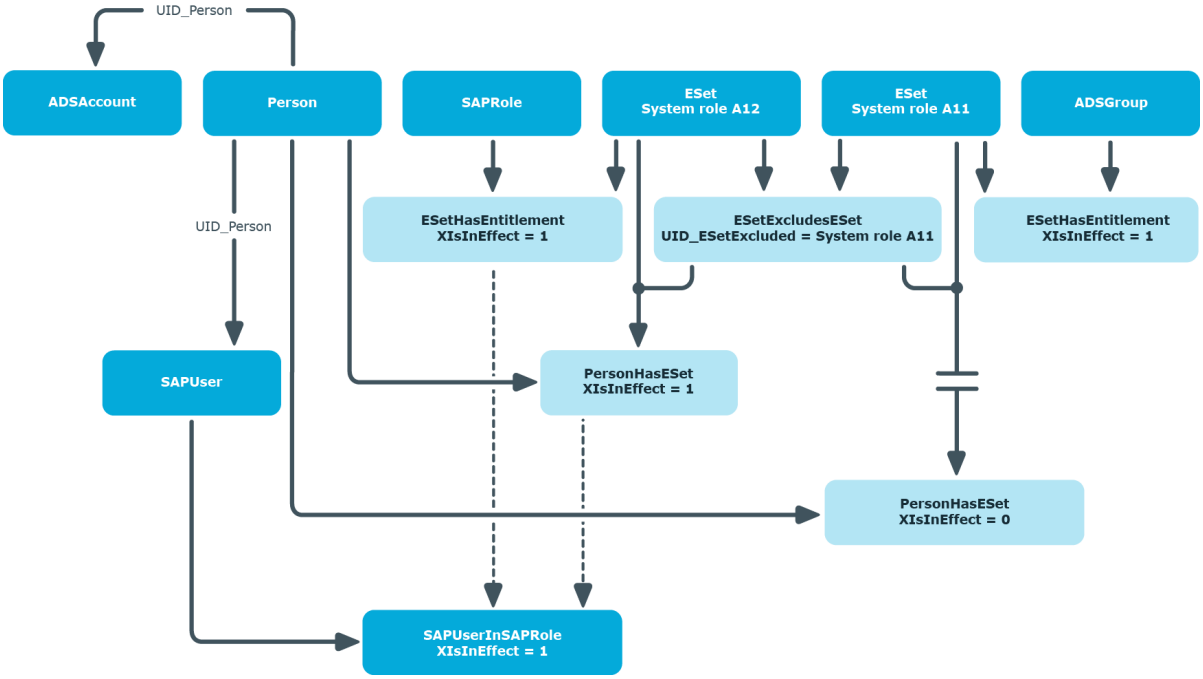
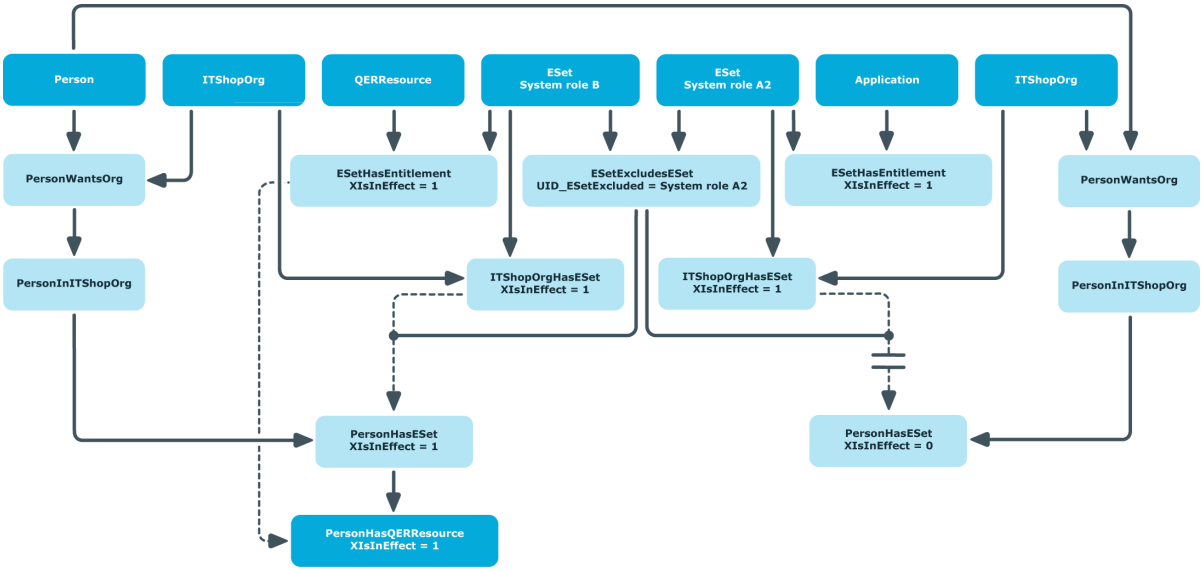


Abbildung 6: Vererbung über eine IT Shop-Bestellung



Besonderheiten bei der Vererbung von Systemrollen über hierarchische Rollen

Tabelle 12: Konfigurationsparameter für die Berechnung von Zuweisungen an hierarchische Rollen

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | NoESetSplitting	Angabe, ob die Bestandteile einer Systemrolle bereits an der hierarchischen Rolle aufgelöst werden oder nicht. Bei Aktivierung werden die Systemrollen erst am Ziel der Vererbung in ihre einzelnen Bestandteile zerlegt.

Wenn der Konfigurationsparameter aktiviert ist, werden Systemrollen, die an hierarchische Rollen zugewiesen sind, bei der Vererbungsberechnung nicht aufgelöst. Das heißt, die Zuweisungen von Unternehmensressourcen an hierarchische Rollen werden nicht in die entsprechenden Zuweisungstabellen (`<BaseTree>Has...`) geschrieben. Erst bei der Vererbungsberechnung für Personen werden die Systemrollen aufgelöst, deren Zuweisungen wirksam sind (`PersonHasESet.XIsIneffect = 1`).

HINWEIS: Eine Systemrollenhierarchie wird immer aufgelöst. Das heißt, die Zuweisung von untergeordneten Systemrollen an hierarchische Rollen wird immer in die Zuweisungstabellen geschrieben. Dieses Verhalten ist unabhängig von der Stellung des Konfigurationsparameters.

Der Konfigurationsparameter ist standardmäßig aktiviert.

Abbildung 7: Vererbung über indirekt zugewiesene Systemrollen bei aktiviertem Konfigurationsparameter

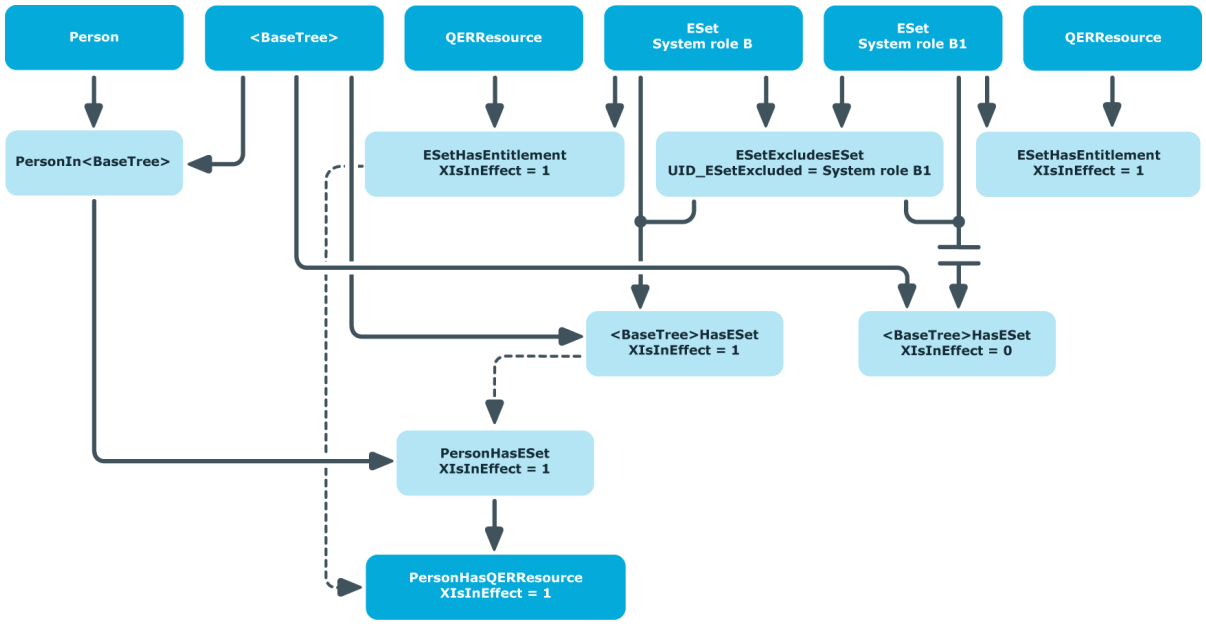
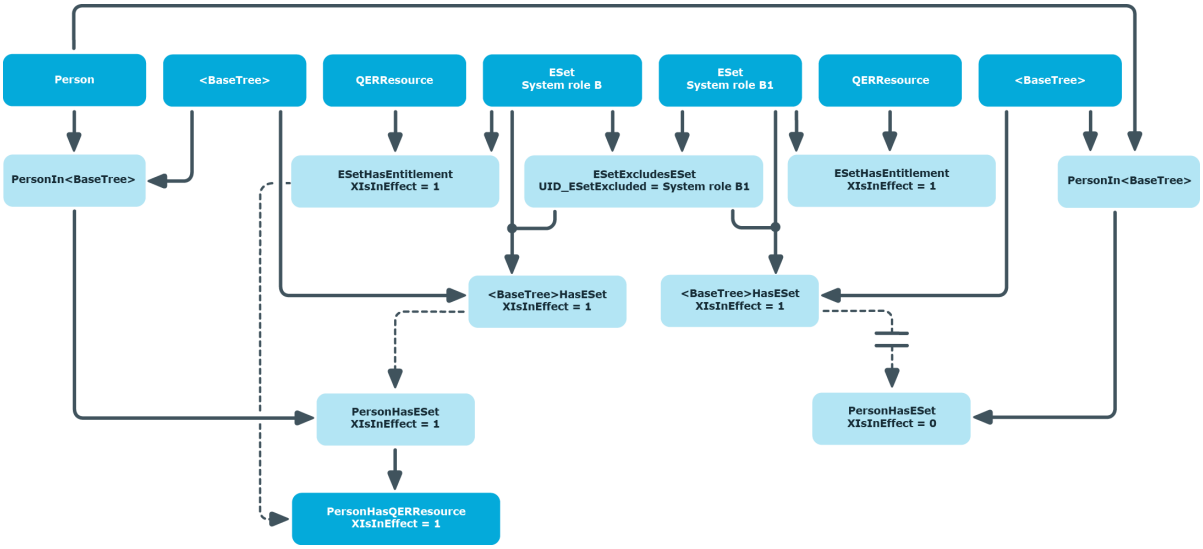
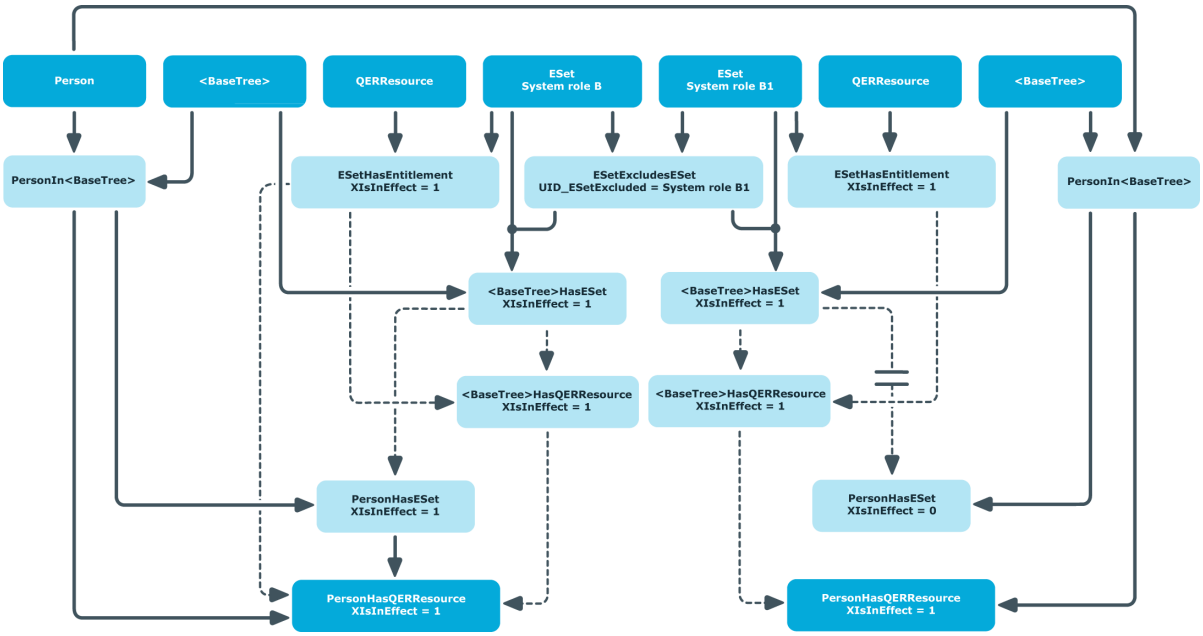


Abbildung 8: Vererbung über unterschiedliche hierarchische Rollen bei aktiviertem Konfigurationsparameter



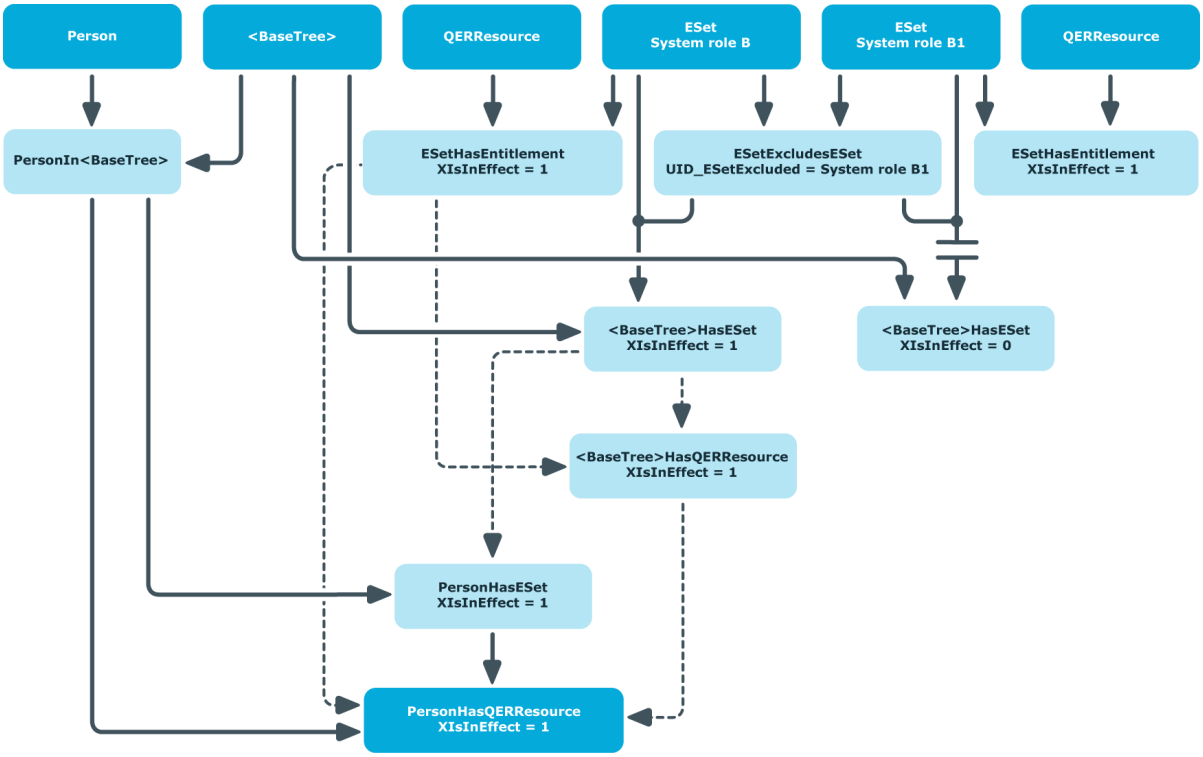
Wenn der Konfigurationsparameter nicht aktiviert ist, werden bei der Vererbungsberechnung für die hierarchischen Rollen die Systemrollen aufgelöst, deren Zuweisungen wirksam sind (`BaseTreeHasESet.XIsIneffect = 1`). Wenn die sich ausschließenden Systemrollen an unterschiedliche hierarchische Rollen zugewiesen sind, sind beide Zuweisungen wirksam. Damit sind auch die daraus resultierenden Zuweisungen der Unternehmensressourcen an die hierarchischen Rollen wirksam. Ist eine Person in beiden hierarchischen Rollen Mitglied, werden dadurch auch die Unternehmensressourcen der ausgeschlossenen Systemrolle an diese Person vererbt.

Abbildung 9: Vererbung über unterschiedliche hierarchische Rollen bei deaktiviertem Konfigurationsparameter



Wenn die sich ausschließenden Systemrollen an dieselbe hierarchische Rolle zugewiesen sind, wirkt die Ausschlussdefinition bereits bei der Berechnung von `BaseTreeHasESet`.

Abbildung 10: Vererbung über dieselbe hierarchische Rolle bei deaktiviertem Konfigurationsparameter



Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

A

Abteilung 20
aktivieren 14
Arbeitsplatz zuweisen 23
Ausgeschlossene Systemrolle 10, 33, 35
Ausschlussdefinition 10, 33

B

bearbeiten 13

D

deaktivieren 14

F

Freigabe 14
Freigabedatum 14

G

Geschäftsrolle 21

I

IT Shop 14, 21

K

Kostenstelle 20

L

Leistungsposition 14

P

Person zuweisen 23

S

Standort 20
Systemrolle 5
  auflösen 35
  ausschließen 10, 26
  in Systemrolle aufnehmen 24
Systemrollenhierarchie 8, 25, 30
Systemrollentyp 14, 16

U

Unternehmensressource 16
  vererben 8, 12, 31

V

Verantwortlicher 14
Vererbung 8
  berechnen 31, 33
  deaktivierte Systemrolle 12
  direkt 31, 33
  indirekt 31, 33, 35
  Systemrolle auflösen 35
  über IT Shop 31, 33

W

Wirksame Systemrolle 10, 26, 33, 35

Z

Zusatzeigenschaft 27