



One Identity Manager 8.1.4

Handbuch zur Autorisierung und Authentifizierung

Copyright 2020 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 Handbuch zur Autorisierung und Authentifizierung
Aktualisiert - 19. Oktober 2020, 07:50 Uhr
Version - 8.1.4

Inhalt

Über dieses Handbuch	7
One Identity Manager Anwendungsrollen	8
Überblick über die Anwendungsrollen	9
Anwendungsrollen für Basisfunktionen	10
Compliance & Security Officer	12
Auditoren	12
Anwendungsrollen für Identity Audit	13
Anwendungsrollen für Unternehmensrichtlinien	14
Anwendungsrollen für Attestierung	16
Anwendungsrolle für abonmierbare Berichte	17
Führungsebene	18
Anwendungsrollen für Geschäftsrollen	18
Anwendungsrollen für Organisationen	19
Anwendungsrollen für Personen	20
Anwendungsrollen für IT Shop	21
Anwendungsrollen für Zielsysteme	23
Anwendungsrollen für das Universal Cloud Interface	24
Anwendungsrollen für benutzerspezifische Aufgaben	25
Inbetriebnahme der Anwendungsrollen	26
Anwendungsrollen erstellen und bearbeiten	27
Stammdaten von Anwendungsrollen	28
Personen an Anwendungsrollen zuweisen	29
Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwen- dungsrollen	30
Zusätzliche Aufgaben für die Verwaltung von Anwendungsrollen	31
Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten	31
Festlegen sich gegenseitig ausschließender Anwendungsrollen	32
Abonmierbare Berichte an Anwendungsrollen zuweisen	33
Zusatzeigenschaften an Anwendungsrollen zuweisen	33
Zuweisungsressourcen für Anwendungsrollen erzeugen	34
Berichte über Anwendungsrollen	34

Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen	36
Vordefinierte Rechtegruppen und Systembenutzer	37
Regeln für die Ermittlung der gültigen Berechtigungen für Tabellen und Spalten	40
Bearbeitung von Rechtegruppen	42
Eigenschaften von Rechtegruppen	43
Abhängigkeiten zwischen Rechtegruppen	44
Abhängigkeiten von Rechtegruppen bearbeiten	45
Rechtegruppen kopieren	46
Rechtegruppen erstellen	47
Bearbeitung von Systembenutzern	48
Systembenutzer erstellen	49
Kennwörter von Systembenutzern	49
Eigenschaften von Systembenutzern	50
Systembenutzer in Rechtegruppen aufnehmen	51
Welche Personen verwenden den Systembenutzer?	52
Dynamische Systembenutzer löschen	53
Bearbeitung der Tabellenrechte und Spaltenrechte	53
Berechtigungen von Rechtegruppen anzeigen	54
Berechtigungen für Tabellen anzeigen	54
Tabellenrechte bearbeiten	55
Spaltenrechte bearbeiten	57
Tabellenrechte und Spaltenrechte kopieren	58
Berechtigungen für Systembenutzer simulieren	59
Berechtigungen für Objekte anzeigen	61
Berechtigungen der angemeldeten Benutzer anzeigen	62
Rollenbasierte Rechtegruppen an Anwendungen zuweisen	63
Steuern von Berechtigungen über Programmfunktionen	64
Programmfunktionen zum Starten der One Identity Manager-Werkzeuge	64
Programmfunktionen des angemeldeten Benutzers anzeigen	67
Programmfunktionen an Rechtegruppen zuweisen	67
Berechtigungen zum Ausführen von Skripten	67
Berechtigungen zum Ausführen von Methoden	68
Berechtigungen zum Auslösen von Prozessen	69
Berechtigungen zum Ausführen von Aktionen im Launchpad	71

One Identity Manager Authentifizierungsmodule	72
Systembenutzer	73
Single Sign-on generisch (rollenbasiert)	73
Person	75
Person (rollenbasiert)	76
Person (dynamisch)	77
Benutzerkonto	78
Benutzerkonto (rollenbasiert)	79
Kontobasierter Systembenutzer	80
Active Directory Benutzerkonto	81
Active Directory Benutzerkonto (rollenbasiert)	82
Active Directory Benutzerkonto (manuelle Eingabe)	83
Active Directory Benutzerkonto (manuelle Eingabe/rollenbasiert)	84
Active Directory Benutzerkonto (dynamisch)	86
LDAP Benutzerkonto (rollenbasiert)	87
LDAP Benutzerkonto (dynamisch)	89
HTTP Header	91
HTTP Header (rollenbasiert)	92
OAuth 2.0/OpenID Connect	93
OAuth 2.0/OpenID Connect (rollenbasiert)	94
Synchronisationsauthenticator	96
Web Agent Authenticator	96
Component Authenticator	97
Crawler	97
Kennworrücksetzung	98
Kennworrücksetzung (rollenbasiert)	99
Bearbeiten der Authentifizierungsmodule	102
Authentifizierungsmodule aktivieren	102
Authentifizierungsmodule zu Anwendungen zuweisen	103
Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren	103
Eigenschaften von Authentifizierungsmodulen	104
Initiale Daten für Authentifizierungsmodule	105
Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers	109
Beispiel für eine einfache Zuordnung zum Systembenutzer	111
Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium	112

Beispiel für eine Zuordnung über Funktionsgruppen	113
Überprüfung der Authentifizierung	114
OAuth 2.0/OpenID Connect Konfiguration	115
Ablauf der OAuth 2.0/OpenID Connect Authentifizierung	115
OAuth 2.0/OpenID Connect Konfiguration erstellen	117
OAuth 2.0/OpenID Connect Konfiguration an Webanwendungen zuweisen	121
Konfiguration des Identitätsanbieters und der OAuth 2.0/OpenID Connect Anwen- dungen anzeigen	122
Aktivierende und deaktivierende Spalten für die Anmeldung festlegen	123
Informationen für OAuth 2.0/OpenID Connect Authentifizierung aufzeichnen	125
Multifaktor-Authentifizierung im One Identity Manager	126
Tabelleneigenschaften bearbeiten	128
Bestellung des Starling 2FA Tokens vorbereiten	129
Sicherheitscode anfordern	129
Entscheidungen über die Starling 2FA App zulassen	131
Abgestufte Berechtigungen für SQL Server und Datenbank	132
Minimale Berechtigungsebenen der One Identity Manager-Werkzeuge	132
Anmeldungen für den Datenbankserver anzeigen	135
Berechtigungsebene des Benutzers anzeigen	135
Berechtigungen der Serverrollen und Datenbankrollen anzeigen	136
Über uns	137
Kontaktieren Sie uns	137
Technische Supportressourcen	137
Index	138

Über dieses Handbuch

Das *One Identity Manager Handbuch zur Autorisierung und Authentifizierung* beschreibt die Grundlagen und Funktionen des One Identity Manager eigenen Rollen- und Berechtigungsmodells.

Dieses Handbuch wurde als Nachschlagewerk für End-Anwender, Systemadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

HINWEIS: Dieses Handbuch beschreibt die Funktionen des One Identity Manager, die für den Standardbenutzer verfügbar sind. Abhängig von der Systemkonfiguration und den Berechtigungen stehen Ihnen eventuell nicht alle Funktionen zur Verfügung.

Sie erhalten einen Überblick über die Standardanwendungsrollen, Standardrechtegruppen und Systembenutzer des One Identity Manager. Sie erfahren, wie Sie die Anwendungsrollen in Betrieb nehmen. Es wird erläutert, wie Sie Berechtigungen auf die Tabellen und Spalten des One Identity Manager Schemas vergeben. Zusätzlich erhalten Sie einen Überblick über die verschiedenen One Identity Manager Authentifizierungsmodule.

Verfügbare Dokumentation

Die One Identity Manager Dokumentation erreichen Sie im Manager und im Designer über das Menü **Hilfe | Suchen**. Die Online Version der One Identity Manager Dokumentation finden Sie im Support-Portal unter [Online-Dokumentation](#). Videos mit zusätzlichen Informationen finden Sie unter www.YouTube.com/OneIdentity.

One Identity Manager Anwendungsrollen

Über das One Identity Manager Rollenmodell werden die Bearbeitungsrechte für die Benutzer des One Identity Manager gesteuert. Das Rollenmodell berücksichtigt sowohl technische Aspekte, zum Beispiel administrative Rechte auf die One Identity Manager-Werkzeuge, als auch funktionale Aspekte, die sich aus den Aufgaben der One Identity Manager Benutzer innerhalb der Unternehmensstruktur ergeben, zum Beispiel die Berechtigung zur Entscheidung von Bestellungen. Der One Identity Manager stellt sogenannte Anwendungsrollen bereit.

Anwendungsrollen erfüllen folgende Ziele:

- Programmfunktionen, Personen, Unternehmensressourcen, Genehmigungsabläufe und Entscheidungsverfahren sind festen Anwendungsrollen zugeordnet. Die Bearbeitungsrechte dieser Anwendungsrollen müssen nicht unternehmensspezifisch festgelegt werden. Damit wird die Administration von Bearbeitungsrechten vereinfacht.
- Es wird eine revisionssichere interne Verwaltung der One Identity Manager Benutzer und ihrer Bearbeitungsrechte ermöglicht. Die Vergabe von Bearbeitungsrechten erfolgt durch Zuordnung, Bestellung und Genehmigung oder durch die Berechnung aufgrund bestimmter Eigenschaften einer Person. Die Plausibilität der Bearbeitungsrechte kann jederzeit über die Attestierungsfunktion geprüft werden.
- Benutzer werden mit den initialen Berechtigungen ausgestattet, die sie zur Erfüllung ihrer Aufgaben benötigen. So können beispielsweise die benötigten Benutzerkonten initial erstellt werden.

Anwendungsrollen können mit Rechtegruppen verknüpft werden, deren Bearbeitungsrechte durch den One Identity Manager vordefiniert sind. Bearbeitungsrechte steuern

- die Gestaltung der Menüführung in den Administrationswerkzeugen,
- den Zugriff auf Objekte und deren Eigenschaften,
- die Anzeige von Oberflächenformularen und Methoden,
- die Verfügbarkeit spezieller Programmfunktionen.

Um die Anwendungsrollen für die Anmeldung am One Identity Manager zu nutzen, müssen die Benutzer ein rollenbasiertes Authentifizierungsmodul verwenden. Rollenbasierte Authentifizierungsmodule ermitteln aus allen Anwendungsrollen des Benutzers die gültigen

Bearbeitungsrechte. Damit erhalten die One Identity Manager Benutzer bei ihrer Anmeldung an den One Identity Manager-Werkzeugen die ihren Anwendungsrollen entsprechenden Berechtigungen auf die Funktionen des One Identity Manager.

Detaillierte Informationen zum Thema

- [Überblick über die Anwendungsrollen](#) auf Seite 9
- [Inbetriebnahme der Anwendungsrollen](#) auf Seite 26
- [Anwendungsrollen erstellen und bearbeiten](#) auf Seite 27

Verwandte Themen

- [Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen](#) auf Seite 36
- [One Identity Manager Authentifizierungsmodule](#) auf Seite 72

Überblick über die Anwendungsrollen

Der One Identity Manager liefert Standardanwendungsrollen mit, deren Berechtigungen auf die verschiedenen Aufgaben und Funktionen abgestimmt sind. Die Personen, die die einzelnen Aufgaben und Funktionen übernehmen, werden an die Standardanwendungsrollen zugewiesen. Zusätzlich können Sie eigene Anwendungsrollen für unternehmensspezifisch definierte Aufgaben erstellen.

HINWEIS: Die Standardanwendungsrollen sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind. Standardanwendungsrollen können nicht gelöscht werden.

Folgende Standardanwendungsrollen sind definiert:

- [Anwendungsrollen für Basisfunktionen](#)
- [Compliance & Security Officer](#)
- [Auditoren](#)
- [Anwendungsrollen für Identity Audit](#)
- [Anwendungsrollen für Unternehmensrichtlinien](#)
- [Anwendungsrollen für Attestierung](#)
- [Anwendungsrolle für abonmierbare Berichte](#)
- [Führungsebene](#)
- [Anwendungsrollen für Geschäftsrollen](#)
- [Anwendungsrollen für Organisationen](#)
- [Anwendungsrollen für Personen](#)
- [Anwendungsrollen für IT Shop](#)

- [Anwendungsrollen für Zielsysteme](#)
- [Anwendungsrollen für das Universal Cloud Interface](#)
- [Anwendungsrollen für benutzerspezifische Aufgaben](#)

Anwendungsrollen für Basisfunktionen

Für Basisfunktionen im One Identity Manager sind die folgenden Anwendungsrollen verfügbar.

Tabelle 1: Anwendungsrollen für Basisfunktionen

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Basisrollen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Administrieren die Anwendungsrollen für Administratoren. • Ordnen Personen in die Anwendungsrollen für Administratoren ein. • Können weitere Personen in die Anwendungsrolle Basisrollen Administratoren aufnehmen und widersprechende Anwendungsrollen bearbeiten. • Sehen die Stammdaten aller übrigen Anwendungsrollen. • Können über das Kennworrücksetzungsportal für ausgewählte Systembenutzer Kennwörter setzen.
Jeder (Ändern)	<p>Die Anwendungsrolle Basisrollen Jeder (Ändern) wird automatisch jedem Benutzer zugewiesen.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Können bestimmte Personenstammdaten im Web Portal bearbeiten. <p>Soll jedem Benutzer bei der Anmeldung automatisch eine kundendefinierte Rechtegruppe zugewiesen werden, so kann diese Rechtegruppe auf dem Stammdatenformular der Anwendungsrolle eingetragen werden.</p> <p>Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.</p>
Jeder (Sehen)	<p>Die Anwendungsrolle Basisrollen Jeder (Sehen) wird automatisch jedem Benutzer zugewiesen.</p> <p>Benutzer mit dieser Anwendungsrolle:</p>

Anwendungsrolle	Beschreibung
	<ul style="list-style-type: none"> • Erhalten Leseberechtigungen auf Objekte im Web Portal. <p>Soll jedem Benutzer bei der Anmeldung automatisch eine kundendefinierte Rechtegruppe zugewiesen werden, so kann diese Rechtegruppe auf dem Stammdatenformular der Anwendungsrolle eingetragen werden.</p> <p>Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.</p>
Personenverantwortliche	<p>Die Anwendungsrolle Basisrollen Personenverantwortliche wird einem Benutzer automatisch zugewiesen, wenn der Benutzer Manager oder Verantwortlicher von Personen, Abteilungen, Standorten, Kostenstellen, Geschäftsrollen oder IT Shops ist.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Bearbeiten die Stammdaten der Objekte, für die sie verantwortlich sind, und weisen ihnen Unternehmensressourcen zu. • Können im Web Portal neue Personen anlegen und die Stammdaten ihrer Mitarbeiter bearbeiten. • Können ihre Mitarbeiter in den IT Shop aufnehmen. • Können im Web Portal die Complianceregelverletzungen ihrer Mitarbeiter sehen. <p>Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.</p>
Initiale Berechtigungen	<p>Die Anwendungsrolle Basisrollen Initiale Berechtigungen wird verwendet, um Personen mit initialen Berechtigungen, die zur Herstellung ihrer Arbeitsfähigkeit notwendig sind, zu versorgen. Der Anwendungsrolle werden alle Ressourcen zugeteilt, die zur automatischen Zuweisung an alle Personen gekennzeichnet sind. Alle internen Personen werden dieser Anwendungsrolle zugewiesen und erhalten die Ressourcen. Die internen Personen werden über eine dynamische Rolle ermittelt.</p>
Betriebsunterstützung	<p>Personen, die das Web Portal für Betriebsunterstützung nutzen, müssen der Anwendungsrolle Basisrollen Betriebsunterstützung zugewiesen werden.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Überwachen die Verarbeitung von Prozessen der Jobqueue. • Überwachen die Verarbeitung der DBQueue.

Anwendungsrolle	Beschreibung
	<ul style="list-style-type: none"> Erstellen Zugangscodes, um Mitarbeitern zu ermöglichen, sich am Kennworrücksetzungsportal anzumelden.
Selbstregistrierte Personen	Der Anwendungsrolle Basisrollen Selbstregistrierte Personen werden alle neuen, externen Personen zugewiesen, die sich im Web Portal selbst registriert haben. Die Personen werden über eine dynamische Rolle ermittelt.

Verwandte Themen

- [Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen](#) auf Seite 30

Compliance & Security Officer

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

Compliance & Security Officer müssen der Anwendungsrolle **Identity & Access Governance | Compliance & Security Officer** zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Sehen im Web Portal alle Compliance-relevanten Informationen und deren Auswertungen. Dazu gehören Attestierungsrichtlinien, Unternehmensrichtlinien und Richtlinienverletzungen, Complianceregeln und Regelverletzungen sowie Risikoindex-Berechnungsvorschriften.
- Können Attestierungsrichtlinien bearbeiten.

Auditoren

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

Die Auditoren sind der Anwendungsrolle **Identity & Access Governance | Auditoren** zugewiesen.

Benutzer mit dieser Anwendungsrolle:

- Sehen im Web Portal alle für ein Audit relevanten Daten.

Anwendungsrollen für Identity Audit

HINWEIS: Diese Anwendungsrollen stehen zur Verfügung, wenn das Modul Compianceregeln vorhanden ist.

Für die Verwaltung von Compianceregeln sind folgende Anwendungsrollen verfügbar.

Tabelle 2: Anwendungsrollen für Identity Audit

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Identity & Access Governance Identity Audit Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Erstellen die Basisdaten für die Erstellung des Regelwerks.• Erstellen die Compianceregeln und weisen die Regelverantwortlichen zu.• Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen.• Erstellen Berichte über Regelverletzungen.• Erfassen risikomindernde Maßnahmen.• Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften.• Überwachen die Identity Audit Funktionen.• Administrieren die Anwendungsrollen für Regelverantwortliche, Ausnahmegenehmiger und Attestierer.• Richten bei Bedarf weitere Anwendungsrollen ein.
Regelverantwortliche	<p>Die Regelverantwortlichen müssen der Anwendungsrolle Identity & Access Governance Identity Audit Regelverantwortliche oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Sind inhaltlich verantwortlich für Compianceregeln, beispielsweise Wirtschaftsprüfer oder Revisionsabteilung.• Bearbeiten die Arbeitskopien der Compianceregeln, denen die Anwendungsrolle zugeordnet ist.• Aktivieren und deaktivieren Compianceregeln.• Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen.• Weisen risikomindernde Maßnahmen zu.

Anwendungsrolle	Beschreibung
Ausnahmegenehmiger	<p>Die Ausnahmegenehmiger müssen der Anwendungsrolle Identity & Access Governance Identity Audit Ausnahmegenehmiger oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Bearbeiten im Web Portal die Regelverletzungen. • Können im Web Portal Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer	<p>Die Attestierer müssen der Anwendungsrolle Identity & Access Governance Identity Audit Attestierer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Attestieren im Web Portal die Complianceregeln und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Complianceregeln sehen, aber nicht bearbeiten. <p>HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.</p>
Pflege SAP Funktionen	<p>Die Administratoren müssen der Anwendungsrolle Identity & Access Governance Identity Audit Pflege SAP Funktionen oder eine untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Sind inhaltlich für die SAP Funktionen verantwortlich. • Bearbeiten die Arbeitskopien der Funktionsdefinitionen, für die sie verantwortlich sind. • Definieren die Funktionsausprägungen und Variablensets für SAP Funktionen. • Weisen risikomindernde Maßnahmen zu. <p>HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul SAP R/3 Compliance Add-on vorhanden ist.</p>

Anwendungsrollen für Unternehmensrichtlinien

HINWEIS: Diese Anwendungsrollen stehen zur Verfügung, wenn das Modul Unternehmensrichtlinien vorhanden ist.

Für die Verwaltung von Unternehmensrichtlinien sind folgende Anwendungsrollen verfügbar.

Tabelle 3: Anwendungsrollen für Unternehmensrichtlinien

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Erstellen die Basisdaten für die Erstellung der Unternehmensrichtlinien. • Erstellen die Richtlinien und weisen die Richtlinienverantwortlichen zu. • Können bei Bedarf die Berechnung der Richtlinien starten und Richtlinienverletzungen einsehen. • Erstellen Berichte über Richtlinienverletzungen. • Erfassen risikomindernde Maßnahmen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Administrieren die Anwendungsrollen für Richtlinienverantwortliche, Ausnahmegenehmiger und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
Richtlinienverantwortliche	<p>Die Richtlinienverantwortlichen müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Richtlinienverantwortliche oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Sind inhaltlich verantwortlich für Unternehmensrichtlinien. • Bearbeiten die Arbeitskopien der Unternehmensrichtlinien. • Aktivieren und deaktivieren Unternehmensrichtlinien. • Können bei Bedarf die Berechnung der Richtlinien starten und Richtlinienverletzungen einsehen. • Weisen risikomindernde Maßnahmen zu.
Ausnahmegenehmiger	<p>Die Ausnahmegenehmiger müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Ausnahmegenehmiger oder</p>

Anwendungsrolle	Beschreibung
	<p>einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Bearbeiten die Richtlinienverletzungen. • Können Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer	<p>Die Attestierer müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Attestierer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Attestieren im Web Portal die Unternehmensrichtlinien und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Unternehmensrichtlinien sehen, aber nicht bearbeiten. <p>HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.</p>

Anwendungsrollen für Attestierung

HINWEIS: Diese Anwendungsrollen stehen zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Für die Verwaltung der Attestierungsverfahren sind folgende Anwendungsrolle verfügbar.

Tabelle 4: Anwendungsrollen für Attestierung

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren sind der Anwendungsrolle Identity & Access Governance Attestierung Administratoren zugewiesen.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Definieren Attestierungsverfahren und Attestierungsrichtlinien. • Erstellen die Entscheidungsrichtlinien und Entscheidungsworkflows. • Legen fest, nach welchen Entscheidungsverfahren die Attestierer ermittelt werden. • Richten die Benachrichtigungen für Attestierungsvorgänge ein.

Anwendungsrolle Beschreibung

	<ul style="list-style-type: none">• Konfigurieren die Zeitpläne für die Attestierungen.• Erfassen risikomindernde Maßnahmen.• Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften.• Überwachen die Attestierungsvorgänge.
Zentrale Entscheidergruppe	<p>Die zentralen Entscheider müssen der Anwendungsrolle Identity & Access Governance Attestierung Zentrale Entscheidergruppe zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Entscheiden über Attestierungsvorgänge.• Weisen Attestierungsvorgänge anderen Attestierern zu.
Attestierer für externe Benutzer	<p>Die Attestierer für externe Benutzer müssen der Anwendungsrolle Identity & Access Governance Attestierung Attestierer für externe Benutzer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Attestieren neue externe Personen.

HINWEIS: Die verantwortlichen Attestierer werden über Entscheidungsverfahren ermittelt. Hierbei können weitere Anwendungsrollen zum Einsatz kommen. Die Anwendungsrollen für Attestierer sind in verschiedenen Modulen definiert und stehen dort zur Verfügung, wenn das Modul Attestierung installiert ist.

Anwendungsrolle für abonnierbare Berichte

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

Für die Verwaltung von abonnierbaren Berichten ist folgende Anwendungsrolle verfügbar.

Tabelle 5: Anwendungsrollen für abonnierbare Berichte

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Identity & Access Governance Abonnierbare Berichte Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Erstellen aus den verfügbaren Berichten die abonnierbaren Berichte.

Anwendungsrolle Beschreibung

- Konfigurieren die Berichtsparameter für abonnierbare Berichte.
- Weisen die abonnierbaren Berichte an Personen, Unternehmensstrukturen oder IT Shop Regale zu.
- Erstellen bei Bedarf kundenspezifische Mailvorlagen zum Versenden abonniertes Berichten per E-Mail.

Führungsebene

Die Benutzer müssen der Anwendungsrolle **Identity Management | Führungsebene** zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Sehen in Web Portal Berichte und Statistiken, die für die Führungsebene Ihres Unternehmens bestimmt sind.

Anwendungsrollen für Geschäftsrollen

HINWEIS: Diese Anwendungsrollen stehen zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Für die Verwaltung der Geschäftsrollen sind folgende Anwendungsrollen verfügbar.

Tabelle 6: Anwendungsrollen für Geschäftsrollen

Anwendungsrolle	Beschreibung
Administratoren	<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.• Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer.• Richten bei Bedarf weitere Anwendungsrollen ein.
Attestierer	<p>Die Attestierer müssen der Anwendungsrolle Identity Management Geschäftsrollen Attestierer oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p>

Anwendungsrolle Beschreibung

Benutzer mit dieser Anwendungsrolle:

- Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Geschäftsrollen, für die sie verantwortlich sind.
- Können die Stammdaten der Geschäftsrollen sehen, aber nicht bearbeiten.

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

Genehmiger

Die Genehmiger müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Genehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Sind Genehmiger für den IT Shop.
- Entscheiden über Bestellungen aus Geschäftsrollen, für die sie verantwortlich sind.

Genehmiger (IT)

Die IT Genehmiger müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Genehmiger (IT)** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Sind IT Genehmiger für den IT Shop.
- Entscheiden über Bestellungen aus Geschäftsrollen, für die sie verantwortlich sind.

Anwendungsrollen für Organisationen

Für die Verwaltung der Abteilungen, Kostenstellen und Standorte sind folgende Anwendungsrollen verfügbar.

Tabelle 7: Anwendungsrollen für Organisationen

Anwendungsrolle Beschreibung

Administratoren

Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Erstellen und Bearbeiten die Abteilungen, Kostenstellen und Standorte.

Anwendungsrolle Beschreibung

- Weisen Unternehmensressourcen an die Abteilungen, Kostenstellen und Standorte zu.
- Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer.
- Richten bei Bedarf weitere Anwendungsrollen ein.

Attestierer

Die Attestierer müssen der Anwendungsrolle **Identity Management | Organisationen | Attestierer** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Attestieren die korrekte Zuweisung von Unternehmensressourcen an die Abteilungen, Kostenstellen und Standorte, für die sie verantwortlich sind.
- Können die Stammdaten der Abteilungen, Kostenstellen und Standorte sehen, aber nicht bearbeiten.

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

Genehmiger

Die Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Sind Genehmiger für den IT Shop.
- Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.

Genehmiger (IT)

Die IT Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger (IT)** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Sind IT Genehmiger für den IT Shop.
- Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.

Anwendungsrollen für Personen

Für die Verwaltung der Personen ist folgende Anwendungsrolle verfügbar.

Tabelle 8: Anwendungsrollen für Personen

Anwendungsrolle	Beschreibung
Administratoren	<p>Personenadministratoren müssen der Anwendungsrolle Identity Management Personen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Bearbeiten die Stammdaten aller Personen.• Ordnen den Manager zu.• Weisen Unternehmensressourcen an die Personen zu.• Überprüfen und autorisieren die Stammdaten von Personen.• Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften.• Bearbeiten Kennwortrichtlinien für Kennwörter von Personen.• Können Sicherheitsschlüssel (Webauthn) von Personen löschen.

Anwendungsrollen für IT Shop

HINWEIS: Diese Anwendungsrollen stehen zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Für die Verwaltung des IT Shop sind folgende Anwendungsrollen verfügbar.

Tabelle 9: Anwendungsrollen für IT Shop

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Request & Fulfillment IT Shop Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Erstellen die IT Shop-Struktur mit Shops, Regalen, Kunden, Vorlagen und dem Servicekatalog.• Erstellen die Entscheidungsrichtlinien und Entscheidungsworkflows.• Legen fest, nach welchen Entscheidungsverfahren die Entscheidung ermittelt werden.• Erstellen die Produkte und Leistungspositionen.• Richten die Benachrichtigungen für Bestellvorgänge ein.• Überwachen die Bestellvorgänge.• Administrieren die Anwendungsrollen für Produkteigner und

Anwendungsrolle Beschreibung

	<p>Attestierer.</p> <ul style="list-style-type: none">• Richten bei Bedarf weitere Anwendungsrollen ein.• Erstellen Zusatzeigenschaften für beliebige Unternehmensressourcen.• Bearbeiten Ressourcen und weisen diese an IT Shop-Strukturen und Personen zu.• Weisen Systemberechtigungen an IT Shop-Strukturen zu.
Produkteigner	<p>Die Produkteigner müssen der Anwendungsrolle Request & Fulfillment IT Shop Produkteigner oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Entscheiden über Bestellungen.• Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind.
Attestierer	<p>Die Attestierer müssen der Anwendungsrolle Request & Fulfillment IT Shop Attestierer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Attestieren die korrekte Zuweisung von Unternehmensressourcen an die IT Shop-Strukturen, für die sie verantwortlich sind.• Können die Stammdaten der IT Shop-Strukturen sehen, aber nicht bearbeiten. <p>HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.</p>
Zentrale Entscheidergruppe	<p>Die zentralen Entscheider müssen der Anwendungsrolle Request & Fulfillment IT Shop Zentrale Entscheidergruppe zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Entscheiden über Bestellungen.• Weisen Bestellungen anderen Entscheidern zu.

HINWEIS: Die verantwortlichen Genehmiger werden über Entscheidungsverfahren ermittelt. Hierbei können weitere Anwendungsrollen zum Einsatz kommen. Die Anwendungsrollen für Genehmiger sind in verschiedenen Modulen definiert und stehen dort zur Verfügung.

Anwendungsrollen für Zielsysteme

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

Für die Verwaltung der Zielsysteme sind folgende Anwendungsrollen verfügbar.

Tabelle 10: Anwendungsrollen für Zielsysteme

Benutzer	Aufgaben
Zielsystemadministratoren	<p>Die Zielsystemadministratoren müssen der Anwendungsrolle Zielsysteme Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.• Legen die Zielsystemverantwortlichen fest.• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.• Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen.• Berechtigen weitere Personen als Zielsystemadministratoren.• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme <Zielsystem> oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>HINWEIS: Pro Zielsystem gibt es mindestens eine Standardanwendungsrolle für Zielsystemverantwortliche. Diese Anwendungsrolle stehen zur Verfügung, wenn das Modul für das Zielsystem vorhanden ist.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Übernehmen die administrativen Aufgaben für das Zielsystem.• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.• Bearbeiten Kennwortrichtlinien für das Zielsystem.• Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor.

Benutzer	Aufgaben
	<ul style="list-style-type: none"> • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp Primäre Identität. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
Zielsystemverantwortliche für den Unified Namespace	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme Unified Namespace oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Erhalten eine zielsystemübergreifende Sicht auf die Objekte der angeschlossenen Zielsysteme. • Können zielsystemübergreifende Berichte erstellen. <p>Sind die Benutzer gleichzeitig Zielsystemverantwortliche der zugrunde liegenden Zielsysteme, können Sie diese Zielsysteme über den Unified Namespace verwalten.</p>

Anwendungsrollen für das Universal Cloud Interface

HINWEIS: Die Anwendungsrollen stehen zur Verfügung, wenn das Modul Universal Cloud Interface installiert ist.

Für die Verwaltung von Cloud-Zielsystemen sind folgende Anwendungsrollen verfügbar.

Tabelle 11: Anwendungsrollen für das Universal Cloud Interface

Benutzer	Aufgaben
Cloud-Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Universal Cloud Interface Administratoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Administrieren die Anwendungsrollen für das Universal

Benutzer	Aufgaben
	<p>Cloud Interface.</p> <ul style="list-style-type: none"> • Richten bei Bedarf weitere Anwendungsrollen ein. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Cloud-Anwendung und One Identity Manager. • Bearbeiten im Manager die Cloud-Anwendungen. • Bearbeiten offene, manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken. • Erhalten im Web Portal und im Manager Informationen über die Cloud-Objekte.
Cloud-Operatoren	<p>Die Operatoren müssen der Anwendungsrolle Universal Cloud Interface Operatoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Bearbeiten offene manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.
Cloud-Auditoren	<p>Die Auditoren müssen der Anwendungsrolle Universal Cloud Interface Auditoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Sehen manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.

Anwendungsrollen für benutzerspezifische Aufgaben

Für benutzerspezifische Funktionen und Aufgaben sind folgende Anwendungsrollen verfügbar.

Tabelle 12: Anwendungsrollen für benutzerspezifische Aufgaben

Anwendungsrolle	Beschreibung
Administratoren	<p>Die Administratoren müssen der Anwendungsrolle Benutzerspezifisch Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Administrieren die benutzerspezifischen Anwendungsrollen.

Anwendungsrolle Beschreibung

Anwendungsrolle	Beschreibung
Verantwortliche	<ul style="list-style-type: none">• Richten bei Bedarf weitere Anwendungsrollen für Verantwortliche ein. <p>Die Verantwortlichen müssen der Anwendungsrolle Benutzerspezifisch Verantwortliche oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Übernehmen unternehmensspezifisch definierte Aufgaben im One Identity Manager.• Konfigurieren und Starten die Synchronisation im Synchronization Editor.• Bearbeiten im Manager Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. <p>Sie können diese Anwendungsrolle beispielsweise nutzen, um One Identity Manager Benutzern Bearbeitungsrechte auf kundenspezifische Tabellen oder Spalten zu gewähren. Alle Anwendungsrollen, die Sie hier definieren, müssen ihre Bearbeitungsrechte über kundendefinierte Rechtegruppen erhalten.</p>

Inbetriebnahme der Anwendungsrollen

WICHTIG: Um Anwendungsrollen einzusetzen, müssen Sie eine Person in die Anwendungsrolle **Basisrollen | Administratoren** aufnehmen. Diese Person ist dann berechtigt, weitere Personen an die administrativen Anwendungsrollen des One Identity Manager zuzuweisen.

Diese Aufgabe führen Sie einmalig aus.

Um eine Person initial in die Anwendungsrolle Basisrollen | Administratoren aufzunehmen

1. Melden Sie sich mit einem nicht-rollenbasierten administrativen Benutzer am Manager an.
2. Wählen Sie die Kategorie **Personen | Personen**.
3. Wählen Sie in der Ergebnisliste die Person aus, der die Anwendungsrolle **Basisrollen | Administrator** zugewiesen werden soll.
4. Wählen Sie die Aufgabe **Berechtigten als One Identity Manager Administrator**.

HINWEIS: Sobald Sie die Ansicht im Manager aktualisieren, wird die Aufgabe **Berechtigten als One Identity Manager Administrator** nicht mehr in der Aufgabenansicht angezeigt. Damit kann die Aufgabe nur ausgeführt werden, solange keine Person dieser Anwendungsrolle zugewiesen ist.

Im Laufe der Arbeit mit One Identity Manager kann es vorkommen, dass keine Person mehr der Anwendungsrolle **Basisrollen | Administratoren** zugewiesen ist. Gehen Sie in diesem Fall wie oben beschrieben vor, um dieser Anwendungsrolle erneut eine Person zuzuweisen.

Der One Identity Manager Benutzer mit der Anwendungsrolle **Basisrollen | Administratoren** kann nun weitere Personen in die administrativen Anwendungsrollen aufnehmen und die Stammdaten der Anwendungsrollen bearbeiten.

Verwandte Themen

- [Personen an Anwendungsrollen zuweisen](#) auf Seite 29
- [Anwendungsrollen erstellen und bearbeiten](#) auf Seite 27

Anwendungsrollen erstellen und bearbeiten

Um Anwendungsrollen initial einzurichten, müssen Sie zuerst eine Person in die Anwendungsrolle **Basisrollen | Administratoren** aufnehmen. Diese Person ist berechtigt, weitere Personen in die verschiedenen Anwendungsrollen für Administratoren aufzunehmen. Weitere Informationen finden Sie unter [Inbetriebnahme der Anwendungsrollen](#) auf Seite 26.


Administratoren können die ihnen untergeordneten Anwendungsrollen bearbeiten, weitere Anwendungsrollen einrichten und Personen zuweisen.

HINWEIS: Um Anwendungsrollen zu bearbeiten, melden Sie sich mit einem rollenbasierten Authentifizierungsmodul am Manager an.

Um eine Anwendungsrolle zu bearbeiten

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten der Anwendungsrolle.
4. Speichern Sie die Änderungen.

Um eine neue Anwendungsrolle zu erstellen

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle, unter der Sie eine neue Anwendungsrolle erstellen möchten.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die Stammdaten der Anwendungsrolle.
4. Speichern Sie die Änderungen.

HINWEIS: Standardanwendungsrollen können nicht gelöscht werden.

Verwandte Themen

- [Stammdaten von Anwendungsrollen](#) auf Seite 28
- [Personen an Anwendungsrollen zuweisen](#) auf Seite 29
- [Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen](#) auf Seite 30
- [One Identity Manager Authentifizierungsmodule](#) auf Seite 72

Stammdaten von Anwendungsrollen

Tabelle 13: Eigenschaften von Anwendungsrollen

Eigenschaft	Bedeutung
Anwendungsrolle	Bezeichnung der Anwendungsrolle.
Interner Name	Freitextfeld für eine unternehmensinterne Bezeichnung.
Vollständiger Name	Vollständiger Name der Anwendungsrolle. Wird aus der Bezeichnung der Anwendungsrolle und den übergeordneten Anwendungsrollen automatisch gebildet.
Übergeordnete Anwendungsrolle	Anwendungsrolle, der die bearbeitete Anwendungsrolle untergeordnet ist.
Abteilung, Standort, Kostenstelle	Zusätzliche Informationen für die Definition der Anwendungsrolle. Diese Eingabefelder dienen lediglich zur Information. Sie sagen nichts darüber aus, für welche Abteilung, Kostenstelle oder Standort die Anwendungsrollen zuständig sind.
Manager	Verantwortlicher Manager der Anwendungsrolle.
2. Verantwortlicher	Stellvertretender Manager der Anwendungsrolle.
Rechtegruppe	<p>Rechtegruppe für die Ermittlung der Bearbeitungsrechte bei rollenbasierter Anmeldung. Eine Anwendungsrolle erhält die Bearbeitungsrechte der zugeordneten Rechtegruppe. Ist keine Rechtegruppe zugeordnet, erhält die Anwendungsrolle die Bearbeitungsrechte der übergeordneten Anwendungsrolle.</p> <p>Administratoren können den übrigen Anwendungsrollen kundendefinierte Rechtegruppen zuordnen. Weitere Informationen finden Sie unter Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen auf Seite 30.</p> <p>HINWEIS: Die Rechtegruppen der Standardanwendungsrollen für Administratoren können nicht bearbeitet werden.</p>
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Eigenschaft	Bedeutung
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Zertifizierungsstatus	Zertifizierungsstatus der Anwendungsrolle. Folgende Werte können ausgewählt werden. <ul style="list-style-type: none"> • Neu: Die Anwendungsrolle wurde neu in der One Identity Manager-Datenbank angelegt. • Zertifiziert: Die Stammdaten der Anwendungsrolle wurden durch einen Manager genehmigt. • Abgelehnt: Die Stammdaten der Anwendungsrolle wurden durch einen Manager nicht genehmigt.
Vererbung blockieren	Angabe, ob die Vererbung an dieser Anwendungsrolle unterbrochen wird. Aktivieren Sie diese Option, um die Vererbung von Unternehmensressourcen an untergeordnete Anwendungsrollen zu verhindern.
Dynamische Rollen nicht erlaubt	Angabe, ob für die Anwendungsrolle eine dynamische Rolle erstellt werden darf.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Personen an Anwendungsrollen zuweisen

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

Sind einer Anwendungsrolle keine Personen direkt zugewiesen, dann werden die Personen der übergeordneten Anwendungsrollen vererbt.

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


Um Personen an eine Anwendungsrolle zuzuweisen

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

Personen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

4. Speichern Sie die Änderungen.

Verwandte Themen

- [Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten](#) auf Seite 31

Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen

Für die rollenbasierte Anmeldung benötigen die Anwendungsrollen einen Verweis auf eine Rechtegruppe, in der die Bearbeitungsrechte für den One Identity Manager definiert sind. Eine Anwendungsrolle erhält die Bearbeitungsrechte der zugeordneten Rechtegruppe. Ist keine Rechtegruppe zugeordnet, erhält die Anwendungsrolle die Bearbeitungsrechte der übergeordneten Anwendungsrolle.

Einigen der Standardanwendungsrollen sind bereits Rechtegruppen zugewiesen. Diese Rechtegruppen besitzen die Bearbeitungsrechte auf die Tabellen und Spalten und sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um im Manager und im Web Portal die Anwendungsdaten zu bearbeiten.

Um die Bearbeitungsrechte der Anwendungsrollen Ihren unternehmensspezifischen Erfordernissen anzupassen, können Sie den Anwendungsrollen kundendefinierte Rechtegruppen zuordnen. Damit Benutzer mit diesen Anwendungsrollen alle Funktionen des One Identity Manager wie in der Standardinstallation nutzen können, sorgen Sie dafür, dass Ihre kundendefinierten Rechtegruppen alle Bearbeitungsrechte der Standardrechtegruppen dieser Anwendungsrollen erhalten.

HINWEIS: Über die hierarchische Verknüpfung von Rechtegruppen können Sie die Zusammenstellung der Rechte vereinfachen. Die Rechte hierarchischer Rechtegruppen werden von oben nach unten vererbt. Das heißt, eine Rechtegruppe erhält alle Rechte ihrer übergeordneten Rechtegruppen.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie im Designer eine neue Rechtegruppe.

HINWEIS: Setzen Sie für die Rechtegruppe die Option **Nur für rollenbasierte Anmeldung**.

2. Stellen Sie im Designer die Abhängigkeit der neuen Rechtegruppe zur Standardrechtegruppe der Anwendungsrolle her. Weisen Sie die Standardrechtegruppe als übergeordnete Rechtegruppe zu. Damit vererbt die Standardrechtegruppe ihre Eigenschaften an die neu definierte Rechtegruppe.
3. Vergeben Sie im Designer zusätzliche Bearbeitungsrechte auf Menüeinträge,

Formulare, Tabellen oder Spalten.

4. Ordnen Sie im Manager die neue Rechtegruppe der Anwendungsrolle zu.

Meldet sich ein Benutzer mit einer derart veränderten Anwendungsrolle am Manager oder am Web Portal an, erhält er – zusätzlich zu den Standardrechten dieser Anwendungsrolle – die unternehmensspezifisch definierten Bearbeitungsrechte.

Verwandte Themen

- [Stammdaten von Anwendungsrollen](#) auf Seite 28
- [Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen](#) auf Seite 36

Zusätzliche Aufgaben für die Verwaltung von Anwendungsrollen

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

Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten

Über diese Aufgabe weisen Sie Personen über dynamische Rollen an eine Anwendungsrolle zu. Ausführliche Informationen zur Verwendung dynamischer Rollen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

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

Um eine dynamische Rolle für eine Anwendungsrolle zu erstellen

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Dynamische Rolle erstellen**.
3. Erfassen Sie die erforderlichen Stammdaten. Für dynamische Rollen für Anwendungsrollen gelten folgende Besonderheiten:
 - **Objektklasse:** Wählen Sie **Person**.
 - **Anwendungsrolle:** Diese Angabe ist mit der ausgewählten Anwendungsrolle vorbelegt. Erfüllen die Personenobjekte die Bedingung der dynamischen Rolle, so werden sie Mitglied dieser Anwendungsrolle.

- **Dynamische Rolle:** Die Bezeichnung der dynamischen Rolle wird standardmäßig aus der Objektklasse und dem vollständigen Namen der Anwendungsrolle gebildet.
4. Speichern Sie die Änderungen.

Um eine dynamische Rolle zu bearbeiten

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Überblick über die Anwendungsrolle**.
3. Klicken Sie auf dem Überblickformular im Formularelement **Dynamische Rollen** auf die Bezeichnung der dynamischen Rolle.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Bearbeiten Sie die dynamische Rolle.
6. Speichern Sie die Änderungen.

Verwandte Themen

- [Stammdaten von Anwendungsrollen](#) auf Seite 28

Festlegen sich gegenseitig ausschließender Anwendungsrollen

Es kann erforderlich sein, dass Personen bestimmte Anwendungsrollen nicht gleichzeitig besitzen dürfen. So dürfen beispielsweise Ausnahmegenehmiger für Regelverletzungen nicht gleichzeitig Regelverantwortliche sein. Um dieses Verhalten zu erreichen, können Sie sich gegenseitig ausschließende Anwendungsrollen festlegen. Sie dürfen diese Anwendungsrollen dann nicht mehr an ein und dieselbe Person zuweisen.

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

Um den Vererbungsausschluss zu konfigurieren

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

Um den Vererbungsausschluss für Anwendungsrollen festzulegen

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle, für die Sie einen Vererbungsausschluss definieren möchten.
2. Wählen Sie die Aufgabe **Widersprechende Anwendungsrollen bearbeiten**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Anwendungsrollen zu, die sich mit der gewählten Anwendungsrolle ausschließen.

- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Anwendungsrollen, die sich nicht länger ausschließen.

4. Speichern Sie die Änderungen.

Abonnierbare Berichte an Anwendungsrollen zuweisen

Über diese Aufgabe können Sie abonnierbare Berichte an eine Anwendungsrolle zuweisen. Alle Personen, die in dieser Anwendungsrolle sind, können die Berichte im Web Portal abonnieren. Ausführliche Informationen zu abonnierbaren Berichten finden Sie im *One Identity Manager Administrationshandbuch für Berichtsabonnements*.

HINWEIS:

- Diese Funktion steht zur Verfügung, wenn das Modul Berichtsabonnement vorhanden ist.
- Die Aufgabe ist nur verfügbar, wenn der Anwendungsrolle (oder einer übergeordneten Anwendungsrolle) eine Rechtegruppe zugeordnet ist.
- Abonnierbare Berichte können nicht an die Anwendungsrollen **Basisrollen | Personenverantwortliche, Basisrollen | Jeder (Sehen)** und **Basisrollen | Jeder (Ändern)** zugewiesen werden.

Um abonnierbare Berichte an einen Anwendungsrolle zuzuweisen

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Abonnierbare Berichte zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berichte zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Berichte.
4. Speichern Sie die Änderungen.

Zusatzeigenschaften an Anwendungsrollen 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 zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um Zusatzeigenschaften für eine Anwendungsrolle festzulegen

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
3. 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 .
4. Speichern Sie die Änderungen.

Zuweisungsressourcen für Anwendungsrollen erzeugen

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

Um eine Zuweisungsressource auf eine Anwendungsrolle einzuschränken

1. Wählen Sie im Manager in der Kategorie **One Identity Manager Administration** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Zuweisungsressource erzeugen**.

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

Berichte über Anwendungsrollen

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für Anwendungsrollen stehen folgende Berichte zur Verfügung.

Tabelle 14: Berichte über Anwendungsrollen

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder IT Shop Strukturen , in denen die Personen der ausgewählten Anwendungsrolle ebenfalls Mitglied sind. Ausführliche Informationen zu Analyse von Rollenmitgliedschaften finden Sie im <i>One Identity Manager Administrationshandbuch für das Identity Management Basismodul</i> .
Historische Mitgliedschaften anzeigen	Der Bericht listet alle Mitglieder der ausgewählten Anwendungsrolle und den Zeitraum ihrer Mitgliedschaft auf.

Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen

Die Berechtigungen für den Zugriff auf die Tabellen und Spalten des One Identity Manager Schemas werden im Schema selbst über Rechtegruppen abgebildet. Rechtegruppen können Sie an Systembenutzer und an Anwendungsrollen zuweisen.

Rechtegruppen werden zusätzlich verwendet, um den Zugriff auf die Bestandteile der Benutzeroberfläche wie Menüeinträge, Formulare, Methoden und Programmfunktionen zu steuern. Meldet sich ein Benutzer an den One Identity Manager-Werkzeugen an, so werden abhängig von den Rechtegruppen des ermittelten Systembenutzers die verfügbaren Menüeinträge, Oberflächenformulare und Methoden ermittelt und die für ihn angepasste Benutzeroberfläche geladen. Ausführliche Informationen zur Bearbeitung der Benutzeroberfläche finden Sie im *One Identity Manager Konfigurationshandbuch*.

Der One Identity Manager stellt Rechtegruppen und Systembenutzer mit einer vordefinierten Benutzeroberfläche und Bearbeitungsrechten auf die Tabellen und Spalten des One Identity Manager Schemas bereit. Diese vordefinierten Konfigurationen werden durch die Schemainstallation gepflegt und sind bis auf einige Eigenschaften nicht bearbeitbar.

Detaillierte Informationen zum Thema

- [Vordefinierte Rechtegruppen und Systembenutzer](#) auf Seite 37
- [Regeln für die Ermittlung der gültigen Berechtigungen für Tabellen und Spalten](#) auf Seite 40
- [Bearbeitung von Rechtegruppen](#) auf Seite 42
- [Bearbeitung von Systembenutzern](#) auf Seite 48
- [Bearbeitung der Tabellenrechte und Spaltenrechte](#) auf Seite 53
- [Steuern von Berechtigungen über Programmfunktionen](#) auf Seite 64
- [Berechtigungen für Objekte anzeigen](#) auf Seite 61
- [Berechtigungen der angemeldeten Benutzer anzeigen](#) auf Seite 62
- [Rollenbasierte Rechtegruppen an Anwendungen zuweisen](#) auf Seite 63

Verwandte Themen

- [One Identity Manager Anwendungsrollen](#) auf Seite 8
- [One Identity Manager Authentifizierungsmodule](#) auf Seite 72

Vordefinierte Rechtegruppen und Systembenutzer

Der One Identity Manager stellt Rechtegruppen und Systembenutzer mit einer vordefinierten Benutzeroberfläche und speziellen Bearbeitungsrechten auf die Tabellen und Spalten des One Identity Manager Schemas bereit. Diese vordefinierten Konfigurationen werden durch die Schemainstallation gepflegt und sind bis auf einige Eigenschaften nicht bearbeitbar.

Tabelle 15: Vordefinierte Rechtegruppen

Rechtegruppe	Beschreibung
Rechtegruppe QBM_BaseRights	Die Rechtegruppe QBM_BaseRights definiert die Basisberechtigungen, die für die Anmeldung eines Systembenutzers an den One Identity Manager-Werkzeugen erforderlich sind. Diese Rechtegruppe ist implizit immer zugewiesen.
Rechtegruppe VID_Features	Die Rechtegruppe VID_Features besitzt alle Programmfunktionen, die zum Starten der One Identity Manager-Werkzeuge erforderlich sind. Zusätzlich besitzt die Rechtegruppe weitere Programmfunktionen zum Ausführen spezieller Funktionen im One Identity Manager.
Rechtegruppe VI_View	Die Rechtegruppe VI_View besitzt die Sichtbarkeitsrechte auf alle Tabellen und Spalten des One Identity Manager-Anwendungsdatenmodells. HINWEIS: Weisen Sie der Rechtegruppe die Sichtbarkeitsrechte auf kundenspezifischen Schemaausweitungen zu.
Rechtegruppe VI_Everyone	Die Rechtegruppe VI_Everyone sind Formularelemente der Übersichtformulare, die Links zu den korrespondierenden Menüeinträgen verwenden, zugewiesen. Zusätzlich stellt diese Rechtegruppen Funktionen für Web Portal Benutzer zur Verfügung. HINWEIS: Weisen Sie die Rechtegruppe ihren kundenspezifischen Systembenutzern zu, damit die Übersichtformulare für den Benutzer vollständig angezeigt werden.

Rechtegruppe	Beschreibung
Rechtegruppen für das One Identity Manager-Anwendungsdatenmodell	Die Rechtegruppen besitzen Bearbeitungsrechte auf die Tabellen und Spalten des One Identity Manager-Anwendungsdatenmodells. Diese Rechtegruppen sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um mit dem Manager die Anwendungsdaten zu bearbeiten.
Rechtegruppen für das One Identity Manager-Systemdatenmodell	Die Rechtegruppen besitzen die Bearbeitungsrechte auf die Tabellen und Spalten des One Identity Manager-Systemdatenmodells. Diese Rechtegruppen sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um Systemdaten zu bearbeiten, beispielsweise mit den Editoren des Designer. Die Rechtegruppe vid besitzt alle Bearbeitungsrechte für die Systemkonfiguration mit dem Designer.
Rollenbasierte Rechtegruppe VI_4_ALLUSER	Die Rechtegruppe VI_4_ALLUSER stellt die Basisberechtigungen sowie Menüeinträge, Formulare, Methode und Programmfunktionen zur Verfügung, um mit dem Manager und dem Web Portal die Anwendungsdaten zu bearbeiten. Diese Rechtegruppe ist implizit immer zugewiesen.
Rollenbasierte Rechtegruppe vi_4_ADMIN_LOOKUP	Die Rechtegruppe vi_4_ADMIN_LOOKUP besitzt die Sichtbarkeitsrechte auf alle Tabellen und Spalten des One Identity Manager-Anwendungsdatenmodells. HINWEIS: Weisen Sie der Rechtegruppe die Sichtbarkeitsrechte auf kundenspezifischen Schemae-rweiterungen zu. Weisen Sie der Rechtegruppe die Sichtbarkeitsrechte auf moduleigene Tabellen und Spalten zu.
Rollenbasierte Rechtegruppe QER_OperationsSupport	Die Rechtegruppe QER_OperationsSupport besitzt spezielle Berechtigungen für die Arbeit mit dem Web Portal für Betriebsunterstützung. Die Rechtegruppe ist der Anwendung OperationsSupportWebPortal zugewiesen. Die Berechtigungen der Rechtegruppe gelten nur im Web Portal für Betriebsunterstützung.
Rollenbasierte Rechtegruppen	Rollenbasierte Rechtegruppen besitzen Bearbeitungsrechte auf die Tabellen und Spalten des One Identity Manager-Anwendungsdatenmodells. Diese Rechtegruppen sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um mit dem Manager und dem Web Portal die Anwendungsdaten zu bearbeiten. Diese Rechtegruppen sind mit One Identity Manager Anwendungsrollen verknüpft und vereinfachen im One Identity Manager Rollenmodell die Administration der Bearbeitungsrechte.

Tabelle 16: Vordefinierte Systembenutzer

Systembenutzer	Beschreibung
Dynamische Systembenutzer	Für die Anmeldung an den One Identity Manager-Werkzeugen mit rollenbasierten Authentifizierungsmodulen werden dynamische Systembenutzer verwendet. Bei der Anmeldung einer Person werden zunächst die Mitgliedschaften der Person in den One Identity Manager Anwendungsrollen ermittelt. Über die Zuordnung der Rechtegruppen zu One Identity Manager Anwendungsrollen wird bestimmt, welche Rechtegruppen für die Person gültig sind. Aus diesen Rechtegruppen wird ein dynamischer Systembenutzer berechnet, der für die Anmeldung der Person benutzt wird.
Systembenutzer sa	Der Systembenutzer sa wird ausschließlich durch den One Identity Manager Service verwendet. Der Systembenutzer ist keiner Rechtegruppe zugeordnet, besitzt jedoch alle Bearbeitungsrechte, Methoden und Programmfunktionen.
Systembenutzer viadmin	<p>Der Systembenutzer viadmin ist der Standard-Systembenutzer des One Identity Manager. Dieser Systembenutzer kann zum Kompilieren einer initialen One Identity Manager-Datenbank und zur ersten Anmeldung an den Administrationswerkzeugen genutzt werden.</p> <p>WICHTIG: Verwenden Sie den Systembenutzer viadmin nicht im produktiven Betrieb. Erstellen Sie einen eigenen Systembenutzer mit entsprechenden Berechtigungen.</p> <p>Der Systembenutzer hat die kompletten vorgegebenen Berechtigungen und die komplette Benutzeroberfläche. Der Systembenutzer erhält implizit die Berechtigungen und Benutzeroberflächenanteile der kundenspezifischen Rechtegruppen. Der Systembenutzer hat die Berechtigung, eine Person als One Identity Manager Administrator für die rollenbasierte Anmeldung einzurichten. Er ist selbst jedoch nicht Mitglied der Anwendungsrollen.</p>
Systembenutzer Synchronization	Der Systembenutzer Synchronization hat die vorgegebenen Berechtigungen, um Zielsystemsynchronisationen über einen Anwendungsserver einrichten und ausführen zu können.
Systembenutzer viHelpdesk	Der Systembenutzer viHelpdesk hat die vorgegebenen Berechtigungen und die Benutzeroberfläche, um mit dem Manager auf die Helpdesk-Ressourcen des One Identity Manager zuzugreifen.

Verwandte Themen

- [Dynamische Systembenutzer löschen](#) auf Seite 53
- [Abhängigkeiten zwischen Rechtegruppen](#) auf Seite 44
- [Bearbeitung von Rechtegruppen](#) auf Seite 42

Regeln für die Ermittlung der gültigen Berechtigungen für Tabellen und Spalten

Meldet sich ein Systembenutzer am System an, werden anhand seiner Rechtegruppen die effektiv wirksamen Berechtigungen für die Objekte bestimmt. Bei der Ermittlung der gültigen Rechte werden folgende Regeln angewendet:

- Die Rechte hierarchischer Rechtegruppen werden von oben nach unten vererbt. Das heißt, eine Rechtegruppe erhält alle Rechte ihrer übergeordneten Rechtegruppen.
- Bei hierarchischer Rechtegruppen wird zuerst die Menge der Objekte ermittelt. Anschließend werden die Spaltenberechtigungen zusammengefasst. Damit ergeben sich unter Umständen mehr effektive Berechtigungen als auf den einzelnen Rechtegruppen definiert sind.
- Ein Systembenutzer erhält ein Recht, wenn mindestens eine seiner Rechtegruppen das Recht besitzt (direkt oder geerbt).
- Die einschränkenden Rechtebedingungen aller Rechtegruppen des Systembenutzers werden zusammengefasst und somit eine gültige Bedingung pro Recht zum Anzeigen, Bearbeiten, Einfügen und Löschen eines Objektes ermittelt.
- Durch das System werden fest definierte Sichtbarkeitsrechte auf den Systemanteil des One Identity Manager-Datenmodells vergeben, die für die Anmeldung eines Systembenutzers an den Administrationswerkzeugen ausreichend sind.
- Ein Systembenutzer, der nur Leserechte besitzt, erhält unabhängig von weiteren Rechten nur die Sichtbarkeitsrechte auf die Objekte.
- Werden auf eine Tabelle die Rechte zum Einfügen, Bearbeiten oder Löschen vergeben, werden implizit auch Sichtbarkeitsrechte vergeben.
- Werden auf eine Spalte die Rechte zum Einfügen oder Bearbeiten vergeben, werden implizit die Sichtbarkeitsrechte vergeben.
- Werden Rechte auf eine Tabelle vergeben, so werden implizit Sichtbarkeitsrechte auf die Primärschlüsselspalte der Tabelle vergeben.
- Ist mindestens das Sichtbarkeitsrecht auf eine Fremdschlüsselspalte vergeben, so werden implizit Sichtbarkeitsrechte auf die referenzierte Tabelle, auf die Primärschlüsselspalte und die Spalten, die laut definiertem Anzeigemuster an der referenzierten Tabelle zur Anzeige benötigt werden, vergeben.
- Spalten, die im definiertem Anzeigemuster an der Tabelle zur Anzeige benötigt werden, erhalten implizit Sichtbarkeitsrechte.
- Rechte für Datenbanksichten vom Typ **Proxy** gelten auch für die zugrunde liegenden Tabellen.
- Für Datenbanksichten vom Typ **ReadOnly** gelten unabhängig von weiteren Rechten nur die Sichtbarkeitsrechte.

- Ist eine Tabelle oder Spalte durch Präprozessorbedingungen deaktiviert, werden keine Rechte auf diese Tabellen und Spalten ermittelt; die Tabelle oder Spalte gilt als nicht vorhanden.
- Ist eine Rechtegruppe durch Präprozessorbedingungen deaktiviert, werden Berechtigungen dieser Rechtegruppe nicht berücksichtigt; die Rechtegruppe gilt als nicht vorhanden.

Beispiel für die Rechtezusammensetzung über Rechtegruppen

Nachfolgendes Beispiel zeigt die Rechtezusammensetzung, wenn der Benutzer in den Rechtegruppen direkt zugeordnet ist und keine hierarchische Verbindung der Rechtegruppen besteht.

Ein Systembenutzer erhält über verschiedene Rechtegruppen die Berechtigungen auf die Tabelle ADSAccount.

Rechtegruppe	Sichtbar	Bearbeitbar	Einfügbar	Löschbar
A	1	1	1	1
B	0	0	0	0

Zusätzlich erhält er über diese Rechtegruppen Berechtigungen auf die Tabelle LDAPAccount.

Rechtegruppe	Sichtbar	Bearbeitbar	Einfügbar	Löschbar
A	1	0	0	0
B	1	1	1	0

Somit hat der Systembenutzer effektiv folgende Rechte:

Tabelle	Sichtbar	Bearbeitbar	Einfügbar	Löschbar
ADSAccount	1	1	1	1
LDAPAccount	1	1	1	0

Beispiel für einschränkende Bedingungen

Ein Systembenutzer erhält über verschiedene Rechtegruppen Sichtbarkeitsrechte auf die Tabelle Person.

Rechtegruppe	Bedingung für Sichtbarkeit	Sichtbarkeitsrecht auf Spalten
A		Lastname
B	Lastname like 'B%'	Lastname, Firstname, Entrydate

Rechtegruppe	Bedingung für Sichtbarkeit	Sichtbarkeitsrecht auf Spalten
C	Lastname like 'Be%'	Lastname, Firstname, Gender
D	Lastname like 'D%'	Lastname

Damit ergeben sich folgende Berechtigungen auf die einzelnen Personenobjekte.

Person.Lastname	Sichtbare Spalten
Meier	Lastname
Bischof	Lastname, Firstname, Entrydate
Beyer	Lastname, Firstname, Gender
Dummy	Lastname

Bearbeitung von Rechtegruppen

Der One Identity Manager stellt Rechtegruppen mit einer vordefinierten Benutzeroberfläche und speziellen Bearbeitungsrechten auf die Tabellen und Spalten des One Identity Manager Schemas bereit. In einigen wenigen Fällen kann es notwendig sein, eigene kundenspezifische Rechtegruppen zu definieren. Eigene Rechtegruppen benötigen Sie beispielsweise, wenn:

- die Standardrechtegruppen zu viele Berechtigungen gewähren,
- ausgewählte Standardrechtegruppen zu einer neuer Rechtegruppe zusammengefasst werden sollen,
- zusätzliche rollenbasierte Rechtegruppen für die kundenspezifischen Anwendungsrollen benötigt werden,
- Berechtigungen auf kundenspezifische Anpassungen wie beispielsweise Schemaerweiterungen, Formulare oder Menüstrukturen erforderlich sind.

Bei der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard werden bereits kundenspezifische Rechtegruppen erstellt, die Sie nutzen können.

- Für die nicht-rollenbasierte Anmeldung werden die Rechtegruppen **CCCViewPermissions** und **CCCEditPermissions** erstellt. Administrative Systembenutzer werden automatisch in diese Rechtegruppen aufgenommen.
- Für die rollenbasierte Anmeldung werden die Rechtegruppen **CCCViewRole** und **CCCEditRole** erstellt.

Rechtegruppen werden im Designer in der Kategorie **Berechtigungen | Rechtegruppen** verwaltet. Sie erhalten hier einen Überblick über die Bearbeitungsrechte und die Bestandteile der Benutzeroberfläche, die den einzelnen Rechtegruppen zugewiesen sind. Zusätzlich werden die Systembenutzer abgebildet, die der Rechtegruppe zugewiesen sind.

Rechtegruppen erstellen und bearbeiten Sie im Designer mit dem Benutzer-& Rechtegruppeneditor. Im Benutzer-& Rechtegruppeneditor werden die Rechtegruppen in ihrer Hierarchie dargestellt. Jede Rechtegruppe wird durch ein Rechtegruppenelement repräsentiert. Das Rechtegruppenelement verfügt über einen Tooltip. Der Inhalt des Tooltips setzt sich aus dem Namen und der Beschreibung der Rechtegruppe zusammen.

Folgende Aufgaben können Sie ausführen:

- Bearbeiten der Stammdaten einer Rechtegruppe
- Definieren neuer Abhängigkeiten zwischen Rechtegruppen
- Kopieren einer Rechtegruppe
- Erstellen einer neuen Rechtegruppe

Verwandte Themen

- [Vordefinierte Rechtegruppen und Systembenutzer](#) auf Seite 37
- [Eigenschaften von Rechtegruppen](#) auf Seite 43
- [Abhängigkeiten von Rechtegruppen bearbeiten](#) auf Seite 45
- [Rechtegruppen kopieren](#) auf Seite 46
- [Rechtegruppen erstellen](#) auf Seite 47
- [Steuern von Berechtigungen über Programmfunktionen](#) auf Seite 64

Eigenschaften von Rechtegruppen

Tabelle 17: Eigenschaften einer Rechtegruppe

Eigenschaft	Beschreibung
Rechtegruppe	Name der Rechtegruppe. Kennzeichnen Sie eigene Rechtegruppen mit dem Präfix CCC .
Beschreibung	Nähere Beschreibung zur Aufgabe der Rechtegruppe.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Präprozessorbedingung	Rechtegruppen können Sie mit einer Präprozessorbedingung versehen. Damit ist die Rechtegruppe nur wirksam, wenn die Präprozessorbedingung erfüllt ist.
Binäres Muster der Rechtegruppe	Das binäre Muster der Rechtegruppe dient zur Berechnung der effektiv wirksamen Systembenutzerrechte. Es wird durch den DBQueue Prozessor vergeben.
Nur für rollenbasierte Anmeldung	Diese Gruppe umfasst Berechtigungen, Formularzuweisungen, Menüeinträge und Programmfunktionen zur rollenbasierten Anmeldung. Die Rechtegruppe kann One Identity Manager Anwendungsrollen zugeordnet werden und wird den dynamisch

Eigenschaft

Beschreibung

ermittelten Systembenutzern zugewiesen. Eine direkte Zuweisung an nicht-dynamische Systembenutzer ist nicht zulässig.

HINWEIS: Diese Option steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Verwandte Themen

- [Rechtegruppen kopieren](#) auf Seite 46
- [Rechtegruppen erstellen](#) auf Seite 47

Abhängigkeiten zwischen Rechtegruppen

Über die Abbildung einer hierarchischen Struktur für Rechtegruppen, können Sie erreichen, dass die Berechtigungen und die Bestandteile der Benutzeroberfläche von einer Rechtegruppe an andere Rechtegruppen vererbt werden. Dabei wird innerhalb der Hierarchie von oben nach unten vererbt.

Für die Abhängigkeit von Rechtegruppen gilt:

- Eine rollenbasierte Rechtegruppe kann von rollenbasierten Rechtegruppen und nicht-rollenbasierten Rechtegruppen erben.
- Eine nicht-rollenbasierte Rechtegruppe kann von nicht-rollenbasierten Rechtegruppen erben. Eine nicht-rollenbasierte Rechtegruppe darf nicht von rollenbasierten Rechtegruppen erben.

Beispiel

Es sind zwei Rechtegruppen mit folgenden Berechtigungen und Bestandteilen der Benutzeroberfläche definiert.

Rechtegruppe	Berechtigungen	Benutzeroberfläche
A	Sichtbarkeitsrechte	Menüstruktur und Formulare
B	Bearbeitungsrechte	Methodendefinitionen

Rechtegruppe A ist in der Hierarchie oberhalb der Rechtegruppe B angeordnet und vererbt an die Rechtegruppe B. Somit stehen einem Benutzer der Rechtegruppe B die Sichtbarkeitsrechte und die Bearbeitungsrechte sowie die Menüstruktur, die Formulare und die Methodendefinitionen zur Verfügung.

Verwandte Themen

- [Abhängigkeiten von Rechtegruppen bearbeiten](#) auf Seite 45

Abhängigkeiten von Rechtegruppen bearbeiten

Abhängigkeiten zwischen Rechtegruppen bearbeiten Sie in der hierarchischen Ansicht des Benutzer- & Rechtegruppeneditors. Rechtegruppen die in der Hierarchie weiter oben angeordnet sind, werden in der hierarchischen Ansicht des Benutzer- & Rechtegruppeneditor weiter rechts angeordnet. Bei Auswahl einer Rechtegruppe in der hierarchischen Ansicht werden die Abhängigkeiten zu anderen Rechtegruppen farbig dargestellt und somit die Vererbungsrichtung gekennzeichnet.

Abbildung 1: Abbildung der Rechtegruppenhierarchie (Vererbungsrichtung von rechts nach links)



Tabelle 18: Bedeutung der Farben in der hierarchischen Darstellung

Farbe	Bedeutung
blau	Die ausgewählte Rechtegruppe.
violett	Diese Rechtegruppe ist der ausgewählten Rechtegruppe direkt untergeordnet und erbt von der ausgewählten Rechtegruppe.
hellviolett	Diese Rechtegruppe erbt über die Hierarchie indirekt von der ausgewählten Rechtegruppe.
rot	Diese Rechtegruppe ist der ausgewählten Rechtegruppe direkt übergeordnet und vererbt an die ausgewählte Rechtegruppe.
hellrot	Diese Rechtegruppe vererbt über die Hierarchie indirekt an die ausgewählte Rechtegruppe.
grün	Diese Rechtegruppe erbt oder vererbt nicht an die ausgewählte Rechtegruppe.

Um Abhängigkeiten einer Rechtegruppe festzulegen

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Rechtegruppen**.
2. Wählen Sie die Rechtegruppe und starten Sie den Benutzer- & Rechtegruppeneditor über die Aufgabe **Rechtegruppe bearbeiten**.
3. In der hierarchischen Ansicht der Rechtegruppen wählen Sie die Rechtegruppe und führen Sie eine der folgenden Aktionen aus.

- Wählen Sie das Kontextmenü **Berechtigungen erben von** und wählen Sie die Rechtegruppen, von denen die ausgewählte Rechtegruppe erben soll.
- Wählen Sie das Kontextmenü **Berechtigungen vererben an** und wählen Sie die Rechtegruppen, die in die ausgewählte Rechtegruppe aufgenommen werden sollen. Die ausgewählte Rechtegruppe vererbt ihre Berechtigung an die untergeordneten Rechtegruppen.

Rechtegruppen kopieren

Der Benutzer- & Rechtegruppeneditor stellt einen Assistenten zur Verfügung, um die Bearbeitungsrechte und die Benutzeroberfläche einer bestehenden Rechtegruppe auf eine neue Rechtegruppe kopieren.

Um eine Rechtegruppe zu kopieren

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Rechtegruppen**.
2. Wählen Sie die Rechtegruppe, die Sie kopieren möchten, und starten Sie den Benutzer- & Rechtegruppeneditor über die Aufgabe **Rechtegruppe bearbeiten**.
3. Wählen Sie das Menü **Rechtegruppen | Rechtegruppe kopieren**.
4. Auf der Startseite des Assistenten zum Kopieren von Rechtegruppen klicken Sie **Weiter**.
5. Auf der Seite **Rechtegruppe wählen** erfassen Sie folgende Informationen:
 - **Wählen Sie die Rechtegruppe, die kopiert werden soll:** Die Rechtegruppe ist vorausgewählt.
 - **Name der Kopie:** Name der neuen Rechtegruppe. Es wird bereits ein Name für die Kopie vorgeschlagen. Sie können diesen Namen anpassen. Achten Sie darauf, dass der Name der Rechtegruppe mit dem Präfix **CCC** beginnt.
6. Auf der Seite **Kopieroptionen wählen** legen Sie fest, welche Beziehungen der Rechtegruppe kopiert werden sollen. Sie können mehrere Optionen wählen. Folgende Kopieroptionen stehen zur Auswahl.

Tabelle 19: Kopieroptionen für Rechtegruppen

Option	Beschreibung
Rechte	Aktivieren Sie diese Option, um die Tabellenrechte und Spaltenrechte der gewählten Rechtegruppe auf die neue Rechtegruppe zu kopieren.
Benutzeroberfläche	Aktivieren Sie diese Option, um die Menüeinträge, die Formulare und die Methodendefinitionen der gewählten Rechtegruppe auf die neue Rechtegruppe zu kopieren.
Systembenutzer	Aktivieren Sie diese Option, um die Systembenutzer der

Option	Beschreibung
	<p>gewählten Rechtegruppe in die neue Rechtegruppe aufzunehmen.</p> <p>HINWEIS: Beachten Sie hierbei, dass vordefinierte Systembenutzer nicht in die neue Rechtegruppe aufgenommen werden.</p>

- Um den Kopiervorgang zu starten, klicken Sie **Weiter**.
Der Kopiervorgang kann einige Zeit in Anspruch nehmen.
- Auf der Seite **Kopieren einer Rechtegruppe** werden die einzelnen Kopierschritte und eventuelle Fehlermeldungen dargestellt. Wenn die Kopieraktion abgeschlossen ist, klicken Sie **Weiter**.
- Um den Assistenten zu beenden, klicken Sie auf der letzten Seite **Fertig**.

Verwandte Themen

- [Rechtegruppen erstellen](#) auf Seite 47
- [Eigenschaften von Rechtegruppen](#) auf Seite 43
- [Abhängigkeiten von Rechtegruppen bearbeiten](#) auf Seite 45
- [Systembenutzer in Rechtegruppen aufnehmen](#) auf Seite 51
- [Bearbeitung der Tabellenrechte und Spaltenrechte](#) auf Seite 53

Rechtegruppen erstellen

Um eine Rechtegruppe zu erstellen

- Wählen Sie im Designer die Kategorie **Berechtigungen**.
- Starten Sie den Benutzer- & Rechtegruppeneditor über die Aufgabe **Rechtegruppe anzeigen/bearbeiten**.
- Fügen Sie eine neue Rechtegruppe über das Menü **Rechtegruppen | Neu** ein.
- Bearbeiten Sie die Stammdaten der Rechtegruppe.
- Speichern Sie die Änderungen.

Verwandte Themen

- [Rechtegruppen kopieren](#) auf Seite 46
- [Eigenschaften von Rechtegruppen](#) auf Seite 43
- [Abhängigkeiten von Rechtegruppen bearbeiten](#) auf Seite 45
- [Systembenutzer in Rechtegruppen aufnehmen](#) auf Seite 51

Bearbeitung von Systembenutzern

One Identity Manager stellt verschiedene Systembenutzer bereit, deren Berechtigungen auf die verschiedenen Aufgaben abgestimmt sind. Erstellen Sie bei Bedarf eigene Systembenutzer. Nehmen Sie die Systembenutzer in Rechtegruppen auf und erteilen Sie den Systembenutzern somit Rechte auf die Tabellen und Spalten des One Identity Manager-Datenmodells und stellen die Benutzeroberfläche zur Verfügung.

Die effektiven Berechtigungen des ermittelten Systembenutzers werden nicht im One Identity Manager Schema gespeichert, sondern bei der Anmeldung an den One Identity Manager-Werkzeugen ermittelt und geladen.

Bei der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard erstellen Sie bereits einen administrative Systembenutzer, der in alle nicht-rollenbasierten Rechtegruppen aufgenommen wird und alle Berechtigungen des Standard-Systembenutzers **viadmin** erhält.

Systembenutzer werden im Designer in der Kategorie **Berechtigungen | Systembenutzer** abgebildet. Sie erhalten einen Überblick über die Rechtegruppen, die den einzelnen Systembenutzern zugewiesen sind. Systembenutzer erstellen und bearbeiten Sie im Designer mit dem Benutzer-& Rechtegruppeneditor.

Folgende Aufgaben können Sie ausführen:

- Erstellen neuer Systembenutzer, beispielsweise administrativer Systembenutzer oder Systembenutzer für Dienstkonten
- Konfiguration der Kennworteinstellungen für Systembenutzer
- Aufnehmen eines Systembenutzer in Rechtegruppen
- Ermitteln welche Personen einen Systembenutzer verwenden

HINWEIS: Dynamische Systembenutzer können Sie nicht bearbeiten.

Verwandte Themen

- [Vordefinierte Rechtegruppen und Systembenutzer](#) auf Seite 37
- [Systembenutzer erstellen](#) auf Seite 49
- [Kennwörter von Systembenutzern](#) auf Seite 49
- [Eigenschaften von Systembenutzern](#) auf Seite 50
- [Systembenutzer in Rechtegruppen aufnehmen](#) auf Seite 51
- [Welche Personen verwenden den Systembenutzer?](#) auf Seite 52
- [Dynamische Systembenutzer löschen](#) auf Seite 53

Systembenutzer erstellen

Um einen Systembenutzer zu erstellen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Benutzer- & Rechtegruppeneditor über die Aufgabe **Rechtegruppe anzeigen/bearbeiten**.
3. Fügen Sie einen neuen Systembenutzer über das Menü **Benutzer | Neu** ein.
4. Bearbeiten Sie die Stammdaten des Systembenutzers.
5. Nehmen Sie den Systembenutzer in die Rechtegruppen auf.
6. Speichern Sie die Änderungen.

HINWEIS: Einen administrativen Systembenutzer können Sie im Benutzer- & Rechtegruppeneditor über das Menü **Administrativen Benutzer anlegen** erstellen. Administrative Systembenutzer werden automatisch in alle nicht-rollenbasierten Rechtegruppen aufgenommen.

Verwandte Themen

- [Vordefinierte Rechtegruppen und Systembenutzer](#) auf Seite 37
- [Kennwörter von Systembenutzern](#) auf Seite 49
- [Eigenschaften von Systembenutzern](#) auf Seite 50
- [Systembenutzer in Rechtegruppen aufnehmen](#) auf Seite 51
- [Dynamische Systembenutzer löschen](#) auf Seite 53
- [Welche Personen verwenden den Systembenutzer?](#) auf Seite 52
- [One Identity Manager Authentifizierungsmodule](#) auf Seite 72

Kennwörter von Systembenutzern

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

Passen Sie im Designer die Kennwortrichtlinie bei Bedarf an ihre Anforderungen an. Ausführliche Informationen zur Bearbeitung von Kennwortrichtlinien finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

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

Um zu verhindern, dass Kennwörter beispielsweise für Dienstkonten ablaufen, aktivieren Sie im Designer für die verwendeten Systembenutzer die Option **Kennwort läuft nie ab** (`DialogUser.PasswordNeverExpires`).

Verwandte Themen

- [Eigenschaften von Systembenutzern](#) auf Seite 50

Eigenschaften von Systembenutzern

Tabelle 20: Eigenschaften eines Systembenutzers

Eigenschaft	Beschreibung
Systembenutzer	Name des Systembenutzers zur Anmeldung an den Administrationswerkzeugen.
Kennwort und Kennwortbestätigung	Kennwort, mit dem sich der Systembenutzer an den Administrationswerkzeugen anmeldet.
Letzte Kennwortänderung	Zeitpunkt der letzten Kennwortänderung.
Kennwort läuft nie ab	Angabe, ob das Kennwort abläuft. Aktivieren Sie die Option beispielsweise für Dienstkonten, um zu verhindern, dass das Kennwort abläuft. Die Option überschreibt das maximale Kennwortalter.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Nur Leserechte	Setzen Sie die Option, wenn ein Systembenutzer in allen Rechtegruppen Mitglied ist, jedoch nur Sichtbarkeitsrechte auf die Objekte haben soll. Damit werden alle Änderungsrechte, die der Systembenutzer über Mitgliedschaften in Rechtegruppen erhält, überschrieben.
Anmeldungen	Anmeldungen, mit denen sich der Systembenutzer an den Werkzeugen des One Identity Manager anmelden kann. Tragen Sie die Anmeldungen in der Form: <code>Domäne\Benutzer</code> ein. Diese Informationen werden benötigt, wenn das Authentifizierungsmodul Kontobasierter Systembenutzer zur Anmeldung an den Werkzeugen des One Identity Manager verwendet wird.
Administrativer Benutzer	Angabe, ob es sich um einen administrativen Systembenutzer handelt. Administrative Systembenutzer werden automatisch in alle nicht-rollenbasierten Rechtegruppen aufgenommen. HINWEIS: Einen administrativen Systembenutzer können Sie im Benutzer- & Rechtegruppeneditor über das Menü Administrativen Benutzer anlegen erstellen.

Eigenschaft	Beschreibung
Dienstkonto	Angabe, ob es sich um einen Systembenutzer handelt, der von einem Dienstkonto verwendet wird. Der Systembenutzer ist keiner Rechtegruppe zugeordnet, besitzt jedoch alle Bearbeitungsrechte, Methoden und Programmfunktionen.
Externe Kennwortverwaltung	Angabe, ob das Kennwort des Systembenutzers über ein externes Kennwortverwaltungssystem ermittelt wird. Das Kennwort kann nicht im One Identity Manager geändert werden. Die Ermittlung des Kennwortes für den Systembenutzer muss kundenspezifisch implementiert werden.

Verwandte Themen

- [Kennwörter von Systembenutzern](#) auf Seite 49

Systembenutzer in Rechtegruppen aufnehmen

Nehmen Sie den Systembenutzer in Rechtegruppen auf und erteilen Sie ihm somit Berechtigungen auf die Tabellen und Spalten des One Identity Manager-Datenmodells und stellen ihm die Benutzeroberfläche zur Verfügung.

HINWEIS:

- Systembenutzer können Sie nicht in rollenbasierte Rechtegruppen aufnehmen. Für die rollenbasierte Anmeldung werden dynamische Systembenutzer errechnet.
- Administrative Systembenutzer werden automatisch in alle nicht-rollenbasierten Rechtegruppen aufgenommen.
- Die Rechtegruppe **QBM_BaseRights** definiert die Basisrechte, die für die Anmeldung eines Systembenutzers an den One Identity Manager-Werkzeugen erforderlich sind. Diese Rechtegruppe ist implizit immer zugewiesen.
- Der Systembenutzer **viadmin** hat die kompletten vorgegebenen Berechtigungen und die komplette Benutzeroberfläche. Der Systembenutzer erhält implizit die Berechtigungen und Benutzeroberflächenanteile der kundenspezifischen Rechtegruppen.

Die Mitgliedschaften eines Systembenutzers in Rechtegruppen werden im Benutzer- & Rechtegruppeneditor dargestellt. Über das Menü **Optionen | Rechtegruppenvererbung** können Sie festlegen, ob die direkten und die vererbten Mitgliedschaften in Rechtegruppen für einen Systembenutzer angezeigt werden.

Abbildung 2: Mitgliedschaften in Rechtegruppen eines Systembenutzers

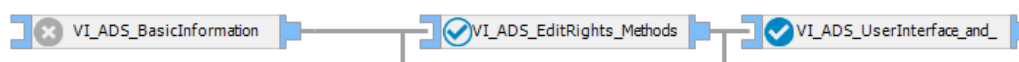






Tabelle 21: Bedeutung der Symbole in der hierarchischen Darstellung

Symbol	Bedeutung
	Der ausgewählte Systembenutzer ist der Rechtegruppe nicht zugeordnet.
	Der ausgewählte Systembenutzer ist der Rechtegruppe direkt zugeordnet.
	Der ausgewählte Systembenutzer ist der Rechtegruppe indirekt zugeordnet.
	Der ausgewählte Systembenutzer ist der Rechtegruppe direkt und indirekt zugeordnet.

Um einen Systembenutzer an eine Rechtegruppe zuzuweisen

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Systembenutzer**.
2. Wählen Sie den Systembenutzer und starten Sie den Benutzer- & Rechtegruppeneditor über die Aufgabe **Systembenutzer bearbeiten**.
3. Wählen Sie in der hierarchischen Ansicht die Rechtegruppe. Per Mausklick auf das Symbol können Sie den ausgewählten Systembenutzer in die Rechtegruppe aufnehmen oder aus der Rechtegruppe entfernen.

TIPP: Um einen Systembenutzer an mehrere Rechtegruppen zuzuweisen, verwenden Sie das Menü **Benutzer | Rechtegruppen** zuweisen.

Verwandte Themen

- [Dynamische Systembenutzer löschen](#) auf Seite 53

Welche Personen verwenden den Systembenutzer?

Personen erhalten einen Systembenutzer direkt über ihre Stammdaten oder dynamisch über ihre One Identity Manager Anwendungsrollen.

Um anzuzeigen, welche Personen einen Systembenutzer verwenden

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Systembenutzer**.
2. Wählen Sie den Systembenutzer und starten Sie den Benutzer- & Rechtegruppeneditor über die Aufgabe **Systembenutzer bearbeiten**.
3. Wählen Sie das Menü **Ansicht | One Identity Manager Personen**.

HINWEIS: Die Zuordnungen können Sie in dieser Ansicht nicht ändern.

Dynamische Systembenutzer löschen

HINWEIS: Erfolgt längere Zeit keine rollenbasierte Anmeldung von Personen, die dynamische Systembenutzer verwenden, sollten Sie die dynamischen Systembenutzer aus Performancegründen löschen. Bei einer späteren rollenbasierten Anmeldung einer Person wird ein dynamischer Systembenutzer neu erzeugt.

Um dynamische Systembenutzer zu löschen

- Aktivieren Sie im Designer den Konfigurationsparameter **Common | DynamicUserLifetime** und geben Sie die maximale Aufbewahrungszeit in Tagen für dynamische Systembenutzer an.

Ist der Konfigurationsparameter aktiviert, werden dynamische Systembenutzer, deren Aufbewahrungszeit abgelaufen sind, im Rahmen der täglichen Wartungsaufträge aus der Datenbank gelöscht.

Bearbeitung der Tabellenrechte und Spaltenrechte

Rechte bearbeiten Sie im Designer mit dem Rechteeditor. Zusätzlich können Sie im Rechteeditor die Berechtigungen für die einzelnen Systembenutzer simulieren.

Mit dem Rechteeditor können Sie:

- Kundenspezifischen Rechtegruppen die Rechte auf kundenspezifische Tabellen und Spalten geben
- Kundenspezifischen Rechtegruppen die Rechte auf vordefinierte Tabellen und Spalten des One Identity Manager Schemas erteilen
- Vordefinierten Rechtegruppen die Rechte auf kundenspezifische Tabellen und Spalten geben

Die Rechte vordefinierter Rechtegruppen auf vordefinierte Tabellen und Spalten des One Identity Manager Schemas können nicht geändert werden.

Bei der kundenspezifischen Schemaerweiterungen mit dem Programm Schema Extension legen Sie eine Rechtegruppe, die Lese- und Schreibrechte erhält sowie eine Rechtegruppe, die nur Leserechte erhält, fest. Damit ist ein erster Zugriff auf die Schemaerweiterungen über die One Identity Manager-Administrationswerkzeuge möglich.

Detaillierte Informationen zum Thema

- [Regeln für die Ermittlung der gültigen Berechtigungen für Tabellen und Spalten auf Seite 40](#)
- [Berechtigungen von Rechtegruppen anzeigen auf Seite 54](#)
- [Berechtigungen für Tabellen anzeigen auf Seite 54](#)

- [Tabellenrechte bearbeiten](#) auf Seite 55
- [Spaltenrechte bearbeiten](#) auf Seite 57
- [Tabellenrechte und Spaltenrechte kopieren](#) auf Seite 58
- [Berechtigungen für Systembenutzer simulieren](#) auf Seite 59

Berechtigungen von Rechtegruppen anzeigen

Um alle Rechte für eine Rechtegruppe anzuzeigen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Rechteeditor über die Aufgabe **Rechte bearbeiten**.
3. Wählen Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** die Rechtegruppe, für die Sie die Rechte anzeigen möchten.

Die Tabellen und Spalten des One Identity Manager Schemas und die Rechte der ausgewählten Rechtegruppe werden im oberen Bereich des Rechteeditors angezeigt. Nutzen Sie die folgenden Optionen des Rechteeditors um die Darstellung anzupassen.

- Um Tabellen mit Rechten zuerst anzuzeigen, aktivieren Sie das Menü **Optionen | Rechte** sortieren.
- Um deaktivierte Tabellen und Spalten anzuzeigen, aktivieren Sie das Menü **Optionen | Deaktivierte Tabellen** anzeigen.
- Um die Anzeigenamen der Tabellen und Spalten zu verwenden, aktivieren Sie das Menü **Optionen | Anzeigenamen verwenden**.
- Um Anzeige der Tabellen einzuschränken, verwenden Sie im Menü **Optionen** die Menüeinträge **Systemtabellen anzeigen**, **Nutzdatentabellen anzeigen** und **Alle Tabellen anzeigen** oder definieren Sie über die Menüeinträge **Filter definieren** oder **Filter verwalten** eigene benutzerdefinierte Filter zur Anzeige der Tabellen und Spalten.

Ausführliche Informationen zum Erstellen von benutzerdefinierten Filtern im Designer finden Sie im *One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge*.

Berechtigungen für Tabellen anzeigen

In der Ansicht **Zusammenfassung aller definierten Rechte** im Rechteeditor werden die Rechtegruppen angezeigt, die Rechte auf eine Tabelle oder Spalte besitzen. Die Rechte sind in dieser Ansicht nicht bearbeitbar.

HINWEIS: Um die Ansicht **Zusammenfassung aller definierten Rechte** anzuzeigen, aktivieren Sie im Rechteeditor das Menü **Ansicht | Objektrechte**. Die Ansicht wird im

unteren Bereich des Rechteeditors angezeigt.

Um alle Rechte für eine Tabelle und ihre Spalten anzuzeigen

1. Wählen Sie im Designer in der Kategorie **Berechtigungen | Nach Tabellen** die Tabelle.
2. Starten Sie den Rechteeditor über die Aufgabe **Rechte auf die Tabelle bearbeiten**.

In der Ansicht **Zusammenfassung aller definierten Rechte** werden die Rechtegruppen angezeigt, die Rechte auf die ausgewählte Tabelle besitzen.

TIPP: Um einen Berechtigungsfilter komplett anzuzeigen, klicken Sie in der Ansicht auf eine Bedingung.

3. (Optional) Um für eine Spalte alle Rechte anzuzeigen, öffnen Sie im oberen Bereich des Rechteeditors den Eintrag für die Tabelle und wählen Sie eine Spalte.

In der Ansicht **Zusammenfassung aller definierten Rechte** werden die Rechtegruppen angezeigt, die Rechte auf die ausgewählte Spalte besitzen.

Tabellenrechte bearbeiten

Über die Tabellenrechten vergeben Sie die Berechtigungen, um die Objekte anzuzeigen, einzufügen, zu bearbeiten und zu löschen. Um die Berechtigungen auf die Objekte weiter einzuschränken, können Sie Bedingungen definieren. Über die Bedingungen können Sie beispielsweise die Bearbeitbarkeit der Personen an deren Nachnamen knüpfen. So kann ein Benutzer auf die Personen deren Nachnamen mit A-F beginnen nur lesend zugreifen, während er die Personen mit Nachnamen von G-Z bearbeiten kann.

HINWEIS: Die Rechte werden im Rechteeditor immer für die Rechtegruppe bearbeitet, die Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** gewählt haben. Wenn Sie Rechte für eine weitere Rechtegruppe vergeben möchten, wählen Sie diese Rechtegruppe zuerst in der Auswahlliste aus und bearbeiten dann die Rechte.

Um für eine Rechtegruppe die Rechte auf eine Tabelle zu bearbeiten

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Rechteeditor über die Aufgabe **Rechte bearbeiten**.
3. Wählen Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** die Rechtegruppe, für die Sie die Rechte vergeben möchten.
4. Wählen Sie im oberen Bereich der Rechteeditors die Tabelle.

TIPP: Mit **Umschalt + Auswahl** oder **Strg + Auswahl** können Sie mehrere Tabellen auswählen.

5. Bearbeiten Sie im Bereich **Rechte** die Rechte für die Rechtegruppe.
 - Um neue Rechte einzufügen, wählen Sie das Kontextmenü **Neu** und aktivieren Sie die zugehörigen Kontrollkästchen. Folgende Rechte können Sie vergeben.

Tabelle 22: Tabellenrechte

Recht	Bedeutung
Sichtbar	Die Datensätze der Tabelle werden angezeigt.
Einfügbar	In die Tabelle können neue Datensätze eingefügt werden.
Bearbeitbar	Die Datensätze der Tabelle können bearbeitet werden
Löschbar	Die Datensätze der Tabelle können gelöscht werden.

HINWEIS: Wenn Sie die Rechte **Einfügbar**, **Bearbeitbar** oder **Löschbar** vergeben, wird auch das Recht **Sichtbar** vergeben.

- Um ein Recht zu entziehen, deaktivieren Sie das zugehörige Kontrollkästchen.
 - Um alle Rechte auf eine Tabelle zu entziehen, verwenden Sie das Kontextmenü **Löschen**.
6. (Optional) Um weitere Bedingungen für Tabellenrechte festzulegen, wechseln Sie im unteren Bereich des Rechteeditors auf die Ansicht **Recht der Rechtegruppe auf Tabelle** und wählen Sie den Tabreiter **Berechtigungsfilter**.

HINWEIS: Berechtigungsfilter können Sie nur auf die Tabellen des Anwendungsdatenmodells definieren.

- Erfassen Sie die Bedingungen als gültige Where-Klausel für Datenbankabfragen. Folgende Berechtigungsfilter können Sie erfassen.

Tabelle 23: Berechtigungsfilter

Berechtigungsfilter	Bedeutung
Bedingung für Sichtbarkeit	Einschränkende Bedingung für die Anzeige der Datensätze.
Bedingung für Bearbeitbarkeit	Einschränkende Bedingung für die Bearbeitung der Datensätze.
Bedingung für Einfügen	Einschränkende Bedingung für das Einfügen der Datensätze.
Bedingung für Löschen	Einschränkende Bedingung für das Löschen der Datensätze.

Beispiel für Berechtigungsfilter

Ein Benutzer soll alle Personen sehen, aber nur die Personen deren Nachname mit B beginnt bearbeiten. Formulieren Sie die

einschränkende Bedingung für die Bearbeitbarkeit beispielsweise folgendermaßen:

```
Lastname like 'B%'
```

TIPP: Mit der Schaltfläche **Überprüfen** können Sie die Bedingung ausführen. Dabei wird die Syntax überprüft. Es wird die Anzahl der Objekte, die der Bedingung entsprechen, zurückgegeben.

Verwandte Themen

- [Spaltenrechte bearbeiten](#) auf Seite 57
- [Tabellenrechte und Spaltenrechte kopieren](#) auf Seite 58

Spaltenrechte bearbeiten

WICHTIG:

- Wenn Sie Rechte auf Spalten vergeben, müssen ebenfalls Sie die Rechte auf die Tabellen vergeben. Beispielsweise ist eine Spalte nur sichtbar, wenn auch die Tabelle sichtbar ist.
- Um Objekte in eine Tabelle einzufügen, benötigen mindestens die Pflichtfelder einer Tabelle das Recht **Einfügbar**.
- Wenn Sie die Rechte **Einfügbar** oder **Bearbeitbar** vergeben, wird auch das Recht **Sichtbar** vergeben.
- Über die Spaltendefinition können Sie Skripte zum bedingten Entfernen des Sichtbarkeitsrechtes oder des Bearbeitungsrechtes für eine Spalte erstellen. Der Rückgabewert **False** entfernt das Recht. Ausführliche Informationen zum Bearbeiten der Spaltendefinitionen finden Sie im *One Identity Manager Konfigurationshandbuch*.

HINWEIS: Die Rechte werden im Rechteeditor immer für die Rechtegruppe bearbeitet, die Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** gewählt haben. Wenn Sie Rechte für eine weitere Rechtegruppe vergeben möchten, wählen Sie diese Rechtegruppe zuerst in der Auswahlliste aus und bearbeiten dann die Rechte.

Um für eine Rechtegruppe die Rechte auf eine Spalte zu bearbeiten

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Rechteeditor über die Aufgabe **Rechte bearbeiten**.
3. Wählen Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** die Rechtegruppe, für die Sie die Rechte vergeben möchten.
4. Wählen Sie im oberen Bereich der Rechteeditors die Tabelle und wählen Sie die

Spalte.

TIPP: Mit **Umschalt + Auswahl** oder **Strg + Auswahl** können Sie mehrere Spalten auswählen.

5. Bearbeiten Sie im Bereich **Rechte** die Rechte für die Rechtegruppe.
 - Um neue Rechte einzufügen, wählen Sie das Kontextmenü **Neu** und aktivieren Sie die zugehörigen Kontrollkästchen. Folgende Rechte können Sie vergeben.

Tabelle 24: Spaltenrechte

Recht	Bedeutung
Sichtbar	Die Spalte wird angezeigt.
Bearbeitbar	Die Werte der Spalte können geändert werden.
Einfügbar	Der Wert der Spalte kann beim Einfügen eines neuen Datensatzes bearbeitet werden. Nach dem Speichern des Datensatzes ist die Spalte nicht mehr bearbeitbar. Es wird beispielsweise beim Erstellen eines Active Directory Benutzers der Active Directory Container festgelegt. Da dieses Feld ein Schlüsselfeld ist, soll der Active Directory Container nach dem Speichern nicht mehr änderbar sein.

- Um ein Recht zu entziehen, deaktivieren Sie das zugehörige Kontrollkästchen.
- Um alle Rechte auf eine Spalte zu entziehen, verwenden Sie das Kontextmenü **Löschen**.

Verwandte Themen

- [Tabellenrechte bearbeiten](#) auf Seite 55
- [Tabellenrechte und Spaltenrechte kopieren](#) auf Seite 58

Tabellenrechte und Spaltenrechte kopieren

Um die Berechtigungen einer Rechtegruppe schnell von einer Tabelle auf andere Tabellen zu übernehmen, können Sie die Tabellenrechte und Spaltenrechte kopieren. Dafür werden im Rechteeditor zwei Methoden angeboten:

- **Kopieren** und **Einfügen**: Mit der Methode werden die Rechte der Quelltable (Quellspalte) einer Rechtegruppe kopiert. Es werden die Rechte der Rechtegruppe kopiert, die Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** gewählt haben.

Es werden alle kopierten Rechte für die Zieltabelle (Zielspalte) eingefügt. Bereits vorhandene Rechte für die Zieltabelle (Zielspalte) bleiben bestehen.

- **Alle Rechte kopieren** und **Alle Rechte einfügen**: Mit der Methode werden die

Rechte der Quelltablette (Quellspalte) kopiert. Die Vorauswahl der Rechtegruppe im Rechteeditor spielt keine Rolle. Es werden die Rechte aller Rechtegruppen der Quelltablette (Quellspalte) übernommen.

Es werden alle kopierten Rechte für die Zieltabelle (Zielspalte) eingefügt. Vorhandene Rechte der Zieltabelle (Zielspalte), die nicht für die Quelltablette (Quellspalte) existieren, werden für die Zieltabelle (Zielspalte) entfernt.

Um die Rechte einer Rechtegruppe zu kopieren

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Rechteeditor über die Aufgabe **Rechte bearbeiten**.
3. Wählen Sie in der Symbolleiste des Rechteeditors in der Auswahlliste **Rechtegruppe** die Rechtegruppe, für die Sie die Rechte vergeben möchten.
4. Um die Tabellenrechte zu übernehmen.
 - a. Wählen Sie im oberen Bereich der Rechteeditors die Tabelle, von der Sie die Rechte übernehmen möchten.
 - b. Kopieren Sie die Rechte über das Kontextmenü **Kopieren** in den Zwischenspeicher.
 - c. Wählen Sie im oberen Bereich der Rechteeditors die Tabelle, für die Sie die Rechte übernehmen möchten.
 - d. Fügen Sie die Rechte über das Kontextmenü **Einfügen** ein.
 - e. Wiederholen bei Bedarf Sie Schritt c) und d) für weitere Tabellen.
5. Um die Spaltenrechte zu übernehmen
 - a. Wählen Sie im oberen Bereich der Rechteeditors die Tabelle und wählen Sie die Spalte, von der Sie die Rechte übernehmen möchten.
 - b. Kopieren Sie die Rechte über das Kontextmenü **Kopieren**.
 - c. Wählen Sie im oberen Bereich der Rechteeditors die Tabelle und wählen Sie die Spalte, für die Sie die Rechte übernehmen möchten.
 - d. Fügen Sie die Rechte über das Kontextmenü **Einfügen** ein.
 - e. Wiederholen bei Bedarf Sie Schritt c) und d) für weitere Spalten.

Verwandte Themen

- [Tabellenrechte bearbeiten](#) auf Seite 55
- [Spaltenrechte bearbeiten](#) auf Seite 57

Berechtigungen für Systembenutzer simulieren

Über die Simulation der Rechte im Rechteeditor sehen Sie für einen Systembenutzer, welche Berechtigungen er aufgrund seiner Rechtegruppen besitzt. Sie können festlegen,

welche Rechtegruppen eines Systembenutzers in die Simulation aufzunehmen sind. Als Ergebnis wird angezeigt, welche der ausgewählten Rechtegruppen, welche Tabellenrechte und Spaltenrechte besitzt. Zusätzlich werden die effektiv wirksamen Berechtigungen für den Systembenutzer dargestellt.

HINWEIS: Der Simulationsmodus ist so lange aktiv bis Sie ihn beenden. Im Simulationsmodus können Sie die Rechte einer Rechtegruppe bearbeiten und die Simulationsdaten aktualisieren.

Um eine Rechtesimulation auszuführen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Rechteeditor über die Aufgabe **Rechte bearbeiten**.
3. Starten Sie über das Menü **Simulation | Simulation starten** den Simulationsassistenten.
4. Auf der Startseite des Assistenten klicken Sie **Weiter**.
5. Auf der Seite **Simulationsbasis wählen** legen Sie folgende Einstellungen fest.
 - **Benutzer:** Wählen Sie den Systembenutzer, für den die Berechtigungen simuliert werden.
 - **direkte Gruppen:** Über diese Schaltfläche wählen Sie alle Rechtegruppen, die dem Systembenutzer direkt zugewiesen sind.
 - **alle Gruppen:** Über diese Schaltfläche wählen Sie alle Rechtegruppen, die dem Systembenutzer direkt zugewiesen sind sowie alle Rechtegruppen, die der Systembenutzer indirekt erbt.
 - **Rechtegruppen:** Wählen Sie einzelne Rechtegruppen direkt aus. Über **Umschalt + Auswahl** können Sie mehrere Tabellen auswählen.
6. Auf der Seite **Simulationskonfiguration** legen Sie fest, für welche Tabellen die Berechtigungen simuliert werden.
 - Im Bereich **Ausgewählte Tabellen** sind alle Tabellen des One Identity Manager Schemas ausgewählt. Schränken Sie die Auswahl bei Bedarf auf einzelne Tabellen ein. Klicken Sie **Keine** um die Auswahl aufzuheben. Wählen Sie mit **Umschalt + Auswahl** einzelne Tabellen aus.
 - Über die Auswahlliste **Kontexttabelle** können Sie eine Tabelle festlegen, aus deren Sicht sich implizite Rechte auf die Anzeigewerte der Fremdschlüsselspalten ergeben.

Beispiel

Für die Tabelle Person wurden Sichtbarkeitsrechte auf die Spalte UID_Org vergeben. Damit werden implizit die Sichtbarkeitsrechte für Spalten der Tabelle Org vergeben, die als Anzeigemuster verwendet werden, beispielsweise Org.Ident_Org.

Wählen Sie für die Simulation dieses Beispiels unter **Kontexttabelle** die Tabelle Person und unter **Ausgewählte Tabellen** die Tabelle Org.

7. Auf der Seite **Simulation** wird der Verarbeitungsfortschritt der Simulation angezeigt. Der Simulationsvorgang kann einige Zeit in Anspruch nehmen.
8. Um den Assistenten zu beenden, klicken Sie auf der letzten Seite **Fertig**.
Nach Abschluss des Simulationsassistenten werden im oberen Bereich des Rechteeditors im Bereich **Simulation** die effektiven Tabellenrechte und Spaltenrechte des Systembenutzers angezeigt.
9. Um zu ermitteln, aus welchen Rechtegruppen des Systembenutzers, welches Tabellenrecht oder Spaltenrecht resultiert, wählen Sie die Tabelle oder Spalte im oberen Bereich des Rechteeditors.
Im unteren Bereich des Rechteeditors werden in der Ansicht **Simulation der Rechte** die Berechtigungen und Rechtegruppen angezeigt.
10. Um den Simulationsmodus zu beenden, wählen Sie das Menü **Simulation | Simulation beenden**.
Die Simulationsdaten werden gelöscht und die Ansicht **Simulation der Rechte** wird geschlossen.

Berechtigungen für Objekte anzeigen

In den One Identity Manager-Werkzeugen können Sie die Eigenschaften und Berechtigungen für Objekte anzeigen.




Um erweiterte Eigenschaften eines Objektes anzuzeigen

- Wählen Sie das Objekt und öffnen Sie das Kontextmenü **Eigenschaften**.

Auf dem Tabreiter **Allgemein** sehen Sie allgemeine Eigenschaften des Objektes, wie beispielsweise Bezeichnung, Status oder Primärschlüssel.

Auf dem Tabreiter **Eigenschaften** werden alle Spalten des Objektes mit ihren Werten in tabellarischer Form angezeigt. Hier können Sie zwischen der einfachen Ansicht der Spalten und der erweiterten Ansicht mit zusätzlichen Angaben zur Spaltendefinition wählen.

Tabelle 25: Verwendete Symbole für Spalteneigenschaften

Symbol	Bedeutung
	Pflichtfeld.
	Keine Sichtbarkeitsrechte vorhanden.
	Keine Bearbeitungsrechte vorhanden.

Auf dem Tabreiter **Rechte** sehen Sie aufgrund welcher Rechtegruppen welche Berechtigungen auf ein Objekt gelten. Der erste Eintrag zeigt die grundlegenden Berechtigungen auf die Tabelle. Darunter sind die Rechte auf das konkrete Objekt aufgelistet. Die weiteren Einträge zeigen die Spaltenrechte an.

TIPP: Doppelklicken Sie auf den Tabelleneintrag, den Objekteintrag oder einen Spalteneintrag, um die Rechtegruppen anzuzeigen, aus denen die Berechtigungen ermittelt wurden.

Tabelle 26: Verwendete Symbole für Berechtigungen

Symbol	Bedeutung
✓	Berechtigung vorhanden.
•	Berechtigung wurde durch die Objektschicht entzogen.
☑	Berechtigung über Bedingung eingeschränkt.

Berechtigungen der angemeldeten Benutzer anzeigen

Um Informationen zum angemeldeten Benutzer zu erhalten


- Um weitere Benutzerinformationen anzuzeigen, doppelklicken Sie in der Statuszeile auf das Symbol .

Tabelle 27: Erweiterte Informationen zum angemeldeten Benutzer

Eigenschaft	Bedeutung
Systembenutzer	Bezeichnung des verwendeten Systembenutzers.
Authentifiziert durch	Bezeichnung des Authentifizierungsmoduls, das zur Anmeldung verwendet wird.
UID der Person (UserUID)	Eindeutige Kennung der Person des angemeldeten Benutzers, falls ein personenbezogenes Authentifizierungsmodul zur Anmeldung benutzt wird.
SQL Berechtigungslevel	Berechtigungsebene der verwendeten Datenbankserver-Anmeldung.
Nur Leserechte	Der verwendete Systembenutzer besitzt nur Leserechte. Datenänderungen sind nicht möglich.
Dynamischer Benutzer	Der angemeldete Benutzer verwendet einen dynamischen Systembenutzer. Dynamische Systembenutzer werden eingesetzt, wenn zur Anmeldung ein rollenbasiertes Authentifizierungsmodul benutzt wird.

Eigenschaft	Bedeutung
Bemerkungen	Nähere Beschreibung zum verwendeten Systembenutzer.
Rechtegruppen	Rechtegruppen, die dem Systembenutzer zugewiesen sind. Abhängig von den Rechtegruppen werden die Benutzeroberfläche und die Bearbeitungsrechte zur Verfügung gestellt.
Programmfunktionen	Programmfunktionen, die dem Systembenutzer zugewiesen sind. Abhängig von den Programmfunktionen werden Menüeinträge und Funktionen zur Verfügung gestellt.

Rollenbasierte Rechtegruppen an Anwendungen zuweisen

Wenn Sie eine rollenbasierte Rechtegruppe an eine Anwendung zuweisen, dann gelten die Berechtigungen der Rechtegruppe nur für diese Anwendung. Meldet sich ein Benutzer an der Anwendung an, erhält er die Berechtigungen der Rechtegruppe zusätzlich zu seinen anderen Berechtigungen.

Um eine rollenbasierte Rechtegruppe an eine Anwendung zuzuweisen

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Rechtegruppen | Rollenbasierte Rechtegruppen**.
2. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `DialogGroupInProductLimited`.
3. Wählen Sie im Listeneditor die Rechtegruppe.
4. Weisen Sie in der Bearbeitungsansicht **Anwendung** die Anwendung zu.

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

Steuern von Berechtigungen über Programmfunktionen

Programmfunktionen gehören zum Berechtigungsmodell im One Identity Manager und ermöglichen es, Funktionalitäten zu aktivieren oder zu deaktivieren. Programmfunktionen können nicht einzelnen Benutzern zugewiesen werden, sondern nur Rechtegruppen. Die Menge an definierten Programmfunktionen für einen Benutzer ergibt sich dann aus seinen Rechtegruppen und den darin enthaltenen Programmfunktionen.

Das Starten der One Identity Manager-Werkzeuge ist nur zulässig, wenn der Benutzer die entsprechenden Programmfunktionen besitzt. Zusätzlich sind einige Funktionen in den One Identity Manager-Werkzeugen nur verfügbar, wenn dem angemeldeten Benutzer die entsprechenden Programmfunktionen zugewiesen sind. Dazu gehören beispielsweise der Datenexport aus dem Manager, der Aufruf des SQL Editors im Designer oder die Anzeige der DBQueue Prozessor Informationen in allen Programmen.

Detaillierte Informationen zum Thema

- [Programmfunktionen zum Starten der One Identity Manager-Werkzeuge](#) auf Seite 64
- [Berechtigungen der angemeldeten Benutzer anzeigen](#) auf Seite 62
- [Programmfunktionen an Rechtegruppen zuweisen](#) auf Seite 67
- [Berechtigungen zum Ausführen von Skripten](#) auf Seite 67
- [Berechtigungen zum Ausführen von Methoden](#) auf Seite 68
- [Berechtigungen zum Auslösen von Prozessen](#) auf Seite 69
- [Berechtigungen zum Ausführen von Aktionen im Launchpad](#) auf Seite 71

Programmfunktionen zum Starten der One Identity Manager-Werkzeuge

Das Starten der One Identity Manager-Werkzeuge ist nur zulässig, wenn der Benutzer die entsprechenden Programmfunktionen besitzt. Die folgenden Programmfunktionen erlauben das Starten der One Identity Manager-Werkzeuge.

Um den Benutzern die Programmfunktion zur Verfügung zu stellen

- Prüfen Sie im Designer in der Kategorie **Berechtigungen | Programmfunktionen**, welche Rechtegruppe die erforderliche Programmfunktion besitzt und weisen Sie bei Bedarf die Programmfunktionen an weitere Rechtegruppen zu.
- Für nicht-rollembasierte Anmeldung: Nehmen Sie im Designer in der Kategorie **Berechtigungen | Systembenutzer** den Systembenutzer in die Rechtegruppe auf.
- Für rollembasierte Anmeldung: Stellen Sie sicher, dass der Benutzer der Anwendungsrolle zugewiesen ist, welche die Programmfunktion über ihre Rechtegruppe besitzt.

Tabelle 28: Programmfunktionen zum Starten der One Identity Manager-Werkzeuge

Programmfunktion	Beschreibung
ApplicationStart_Analyzer	Erlaubt das Starten des Programms Analyzer (Analyzer.exe).
ApplicationStart_ApiDesigner	Erlaubt das Starten des Programms API Designer (ApiDesigner.exe).
ApplicationStart_ConfigWizard	Erlaubt das Starten des Programms Configuration Wizard (ConfigWizard.exe).
ApplicationStart_CryptoConfig	Erlaubt das Starten des Programms Crypto Configuration (CryptoConfig.exe).
ApplicationStart_DataImporter	Erlaubt das Starten des Programms Data Import (DataImporter.exe).
ApplicationStart_DBClone	Erlaubt das Starten des Programms DBClone.exe.
ApplicationStart_DBComparer	Erlaubt das Starten des Programms DBComparer.exe.
ApplicationStart_DBCompiler	Erlaubt das Starten des Programms Database Compiler (DBCompiler.exe).
ApplicationStart_Designer	Erlaubt das Starten des Programms Designer (Designer.exe).
ApplicationStart_JobQueueInfo	Erlaubt das Starten des Programms Job Queue Info (JobQueueInfo.exe).
ApplicationStart_LaunchPad	Erlaubt das Starten des Programms Launchpad (LaunchPad.exe).
ApplicationStart_LicenseMeter	Erlaubt das Starten des Programms License Meter (LicenseMeter.exe).
ApplicationStart_Manager	Erlaubt das Starten des Programms Manager (Manager.exe).
ApplicationStart_ObjectBrowser	Erlaubt das Starten des Programms Object Browser (ObjectBrowser.exe).


Programmfunktion	Beschreibung
ApplicationStart_OpSupport	Erlaubt das Starten des Web Portal für Betriebsunterstützung.
ApplicationStart_ReportEdit	Erlaubt das Starten des Programms Report Editor (ReportEdit2.exe).
ApplicationStart_SchemaExtension	Erlaubt das Starten des Programms Schema Extension (SchemaExtension.exe).
ApplicationStart_ServerInstaller	Erlaubt das Starten des Programms Server Installer (ServerInstaller.exe).
ApplicationStart_SoftwareLoader	Erlaubt das Starten des Programms Software Loader (SoftwareLoader.exe).
ApplicationStart_SynchronizationEditor	Erlaubt das Starten des Programms Synchronization Editor (SynchronizationEditor.exe).
ApplicationStart_SystemDebugger	Erlaubt das Starten des Programms System Debugging (SystemDebugger.exe).
ApplicationStart_Transporter	Erlaubt das Starten des Programms Database Transporter (Transporter.exe).
ApplicationStart_WebDesignerCompiler	Erlaubt das Starten des Programms VI.WebDesigner.CompilerCmd.exe.
ApplicationStart_WebConfig	Erlaubt das Starten des Programms Web Designer Configuration Editor (WebConfigEditor.exe).
ApplicationStart_WebDesigner	Erlaubt das Starten des Programms Web Designer (WebDesigner.exe).
ApplicationStart_WebDesignerInstall	Erlaubt das Starten des Programms Web Installer (WebDesigner.Installer.exe).

Verwandte Themen

- [Programmfunktionen an Rechtegruppen zuweisen](#) auf Seite 67
- [Systembenutzer in Rechtegruppen aufnehmen](#) auf Seite 51
- [Personen an Anwendungsrollen zuweisen](#) auf Seite 29

Programmfunktionen des angemeldeten Benutzers anzeigen

Um die verfügbaren Programmfunktionen für den angemeldeten Benutzer zu ermitteln

- Um die Benutzerinformationen anzuzeigen, doppelklicken Sie in der Statuszeile des Programms auf das Symbol .
Auf dem Tabreiter **Programmfunktionen** werden die verfügbaren Programmfunktionen angezeigt.

Programmfunktionen an Rechtegruppen zuweisen

Um eine Programmfunktion an Rechtegruppen zuzuweisen

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
2. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `DialogGroupHasFeature`.
3. Wählen Sie im Listeneditor die Programmfunktion.
4. Weisen Sie in der Bearbeitungsansicht **Rechtegruppen** die Rechtegruppen zu.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Systembenutzer in Rechtegruppen aufnehmen](#) auf Seite 51

Berechtigungen zum Ausführen von Skripten

Die grundlegende Berechtigung zum Ausführen von Skripten erhält der angemeldete Benutzer über die Programmfunktion **Erlaubt das Ausführen von Skripten im Frontend** (`Common_StartScripts`).

Wird ein Skript zusätzlich mit einer Programmfunktion versehen (Tabelle `QBMScriptHasFeature`), so kann ein Benutzer dieses Skript nur noch ausführen, wenn er auch die nötige Programmfunktion über seine Rechtegruppen besitzt. Besitzt der Benutzer die Programmfunktion nicht, so wird beim Ausführungsversuch eine Fehlermeldung geworfen.

Um die Ausführung eines Skriptes über eine Programmfunktion zu steuern

1. Erstellen Sie eine neue Programmfunktion.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Objekt | Neu**.
 - c. Erfassen Sie die folgenden Informationen:
 - **Programmfunktion:** Bezeichnung der Programmfunktion.
 - **Beschreibung:** Kurze Beschreibung der Programmfunktion.
 - **Funktionsgruppe:** Merkmal zu Gruppierung von Programmfunktionen.
2. Verbinden Sie die Programmfunktion mit den Skripten, die die Benutzer auslösen dürfen.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `QBMScriptHasFeature`.
 - c. Wählen Sie im Listeneditor die neu erstellte Programmfunktion.
 - d. Weisen Sie in der Bearbeitungsansicht **Skripte** die Skripte zu.
3. Weisen Sie die Programmfunktion an die kundenspezifische Rechtegruppe zu, deren Systembenutzer die Skripte ausführen sollen.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `DialogGroupHasFeature`.
 - c. Wählen Sie im Listeneditor Ihre neu erstellte Programmfunktion.
 - d. Wählen Sie im Listeneditor mit **Strg + Auswahl** Ihre neu erstellte Programmfunktion und die Programmfunktion **Erlaubt das Ausführen von Skripten im Frontend** (`Common_StartScripts`).
 - e. Weisen Sie in der Bearbeitungsansicht **Rechtegruppen** die Rechtegruppe zu.

Verwandte Themen

- [Bearbeitung von Rechtegruppen](#) auf Seite 42

Berechtigungen zum Ausführen von Methoden

Wird eine Methodendefinition mit einer Programmfunktion (Tabelle `QBMethodHasFeature`) versehen, so kann ein Benutzer diese Methode nur noch ausführen, wenn er auch die nötige

Programmfunktion über seine Rechtegruppen besitzt. Besitzt der Benutzer die Programmfunktion nicht, so wird beim Ausführungsversuch eine Fehlermeldung geworfen.

Um eine Methodendefinition über eine Programmfunktion an Benutzer zur Verfügung zu stellen

1. Erstellen Sie eine neue Programmfunktion.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Objekt | Neu**.
 - c. Erfassen Sie die folgenden Informationen:
 - **Programmfunktion:** Bezeichnung der Programmfunktion.
 - **Beschreibung:** Kurze Beschreibung der Programmfunktion.
 - **Funktionsgruppe:** Merkmal zu Gruppierung von Programmfunktionen.
2. Verbinden Sie die Programmfunktion mit den Methodendefinitionen, die die Benutzer auslösen sollen.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `QBMethodHasFeature`.
 - c. Wählen Sie im Listeneditor die neu erstellte Programmfunktion.
 - d. Weisen Sie in der Bearbeitungsansicht **Methoden** die Methodendefinitionen zu.
3. Weisen Sie die Programmfunktion an die kundenspezifische Rechtegruppe zu, deren Systembenutzer die Methoden ausführen sollen.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `DialogGroupHasFeature`.
 - c. Wählen Sie im Listeneditor Ihre neu erstellte Programmfunktion.
 - d. Weisen Sie in der Bearbeitungsansicht **Rechtegruppen** die Rechtegruppe zu.

Verwandte Themen

- [Bearbeitung von Rechtegruppen](#) auf Seite 42

Berechtigungen zum Auslösen von Prozessen

Die grundlegende Berechtigung zum Auslösen von Prozessen erhält der angemeldete Benutzer über die Programmfunktion **Erlaubt das Auslösen von Ereignissen im**

Frontend (Common_TriggerEvents).

Im One Identity Manager ist das Auslösen von Ereignissen an den hinterlegten Prozessen mit dem Berechtigungskonzept verbunden. Benutzer dürfen nur an solchen Objekten Ereignisse auslösen, für die Sie auch Bearbeitungsrechte besitzen. Dies kann dazu führen, dass Benutzer an Tabellen, für die nur Sichtbarkeitsrechte definiert sind, keine zusätzlichen Ereignisse für Prozesse auslösen können.

Für diesen Fall gibt es die Möglichkeit die Objekteignisse (Tabelle QBMEvent) mit einer Programmfunktion (Tabelle QBMFeature) zu verbinden. Ein Ereignis (Tabelle JobEventGen), welches für einen Prozess definiert wird, wird mit einem Objekteignis (Spalte JobEventGen.UID_QBMEvent) verknüpft. Wird das Objekteignis mit einer Programmfunktion (Tabelle QBMEventHasFeature) versehen, dann können Benutzer, die diese Programmfunktion über ihre Rechtegruppen besitzen, das Objekteignis und damit auch den Prozess auslösen, unabhängig von ihren Berechtigungen.

Um das Auslösen eines Prozesses über eine Programmfunktion zu steuern

1. Erstellen Sie eine neue Programmfunktion.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Objekt | Neu**.
 - c. Erfassen Sie die folgenden Informationen:
 - **Programmfunktion:** Bezeichnung der Programmfunktion.
 - **Beschreibung:** Kurze Beschreibung der Programmfunktion.
 - **Funktionsgruppe:** Merkmal zu Gruppierung von Programmfunktionen.
2. Verbinden Sie die Programmfunktion mit den Objekteignissen, die die Benutzer auslösen sollen.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle QBMEventHasFeature.
 - c. Wählen Sie im Listeneditor die neu erstellte Programmfunktion.
 - d. Weisen Sie in der Bearbeitungsansicht **Objekteignisse** die Objekteignisse zu.
3. Weisen Sie die benötigten Programmfunktionen an die kundenspezifische Rechtegruppe zu, deren Systembenutzer die Ereignisse auslösen sollen.
 - a. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
 - b. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle DialogGroupHasFeature.
 - c. Wählen Sie im Listeneditor mit **Strg + Auswahl** Ihre neu erstellte Programmfunktion und die Programmfunktion **Erlaubt das Auslösen von**

Ereignissen im Frontend (Common_TriggerEvents).

d. Weisen Sie in der Bearbeitungsansicht **Rechtegruppen** die Rechtegruppe zu.

Verwandte Themen

- [Bearbeitung von Rechtegruppen](#) auf Seite 42

Berechtigungen zum Ausführen von Aktionen im Launchpad

One Identity Manager liefert eine Reihe von Launchpad Aktionen, die Sie zum Starten von Anwendungen über das Launchpad verwenden können. Bei Bedarf können Sie auch eigene Anwendungen über Launchpad Aktionen starten.

Sollen Aktionen im Launchpad nicht für alle Benutzer verfügbar sein, steuern Sie die Berechtigungen über die Zuweisung von Launchpad Aktionen an Programmfunktionen (Tabelle QBMLaunchActionHasFeature). Es werden nur die Aufgaben im Launchpad angezeigt, deren Aktionen ein Benutzer über seine Programmfunktion ausführen darf.

Um eine Programmfunktion an Launchpad Aktionen zuzuweisen

1. Wählen Sie im Designer die Kategorie **Berechtigungen | Programmfunktionen**.
2. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle QBMLaunchActionHasFeature.
3. Wählen Sie im Listeneditor die Programmfunktion.
4. Weisen Sie in der Bearbeitungsansicht **Launchpad Aktionen** die Aktionen zu.
5. Speichern Sie die Änderungen.

One Identity Manager Authentifizierungsmodule

Zur Anmeldung an den Administrationswerkzeugen verwendet der One Identity Manager unterschiedliche Authentifizierungsmodule. Die Authentifizierungsmodule ermitteln den anzuwendenden Systembenutzer und laden abhängig von dessen Mitgliedschaften in Rechtegruppen die Benutzeroberfläche und die Bearbeitungsrechte auf Ressourcen der Datenbank.

- Für die Anmeldung an den One Identity Manager-Werkzeugen mit einem Authentifizierungsmodul, das einen definierten Systembenutzer erwartet, werden die Berechtigungen aus den Rechtegruppen ermittelt, die dem Systembenutzer zugewiesen sind.
- Für die Anmeldung an den One Identity Manager-Werkzeugen mit rollenbasierten Authentifizierungsmodulen werden dynamische Systembenutzer verwendet. Bei der Anmeldung einer Person werden zunächst die Mitgliedschaften der Person in den One Identity Manager Anwendungsrollen ermittelt. Über die Zuordnung der Rechtegruppen zu One Identity Manager Anwendungsrollen wird bestimmt, welche Rechtegruppen für die Person gültig sind. Aus diesen Rechtegruppen wird ein dynamischer Systembenutzer berechnet, der für die Anmeldung der Person benutzt wird.

Um ein Authentifizierungsmodul zur Anmeldung zu verwenden, sind folgende Voraussetzungen zu erfüllen:

1. Das Authentifizierungsmodul muss aktiviert sein.
2. Das Authentifizierungsmodul muss der Anwendung zugewiesen sein.
3. Die Zuweisung des Authentifizierungsmoduls zur Anwendung muss aktiviert sein.

Damit ist die Anmeldung mit diesem Authentifizierungsmodul an den zugewiesenen Anwendungen möglich. Stellen Sie sicher, dass die Benutzer, die durch das Authentifizierungsmodul ermittelt werden, auch die benötigten Programmfunktionen besitzen, die Anwendung zu benutzen.

HINWEIS: Nach der initialen Schemainstallation sind im One Identity Manager nur die Authentifizierungsmodule **Systembenutzer** und **Component Authenticator** sowie die rollenbasierten Authentifizierungsmodule aktiviert.

Für die Anmeldung am Designer verwenden Sie nicht-rollenbasierte Authentifizierungsmodule. Rollenbasierte Authentifizierungsmodule werden für die Anmeldung am Designer nicht unterstützt.

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

Systembenutzer

Anmeldeinformationen	Bezeichnung und Kennwort des Systembenutzers.
Voraussetzungen	<ul style="list-style-type: none">• Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden.
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	nein
Bemerkungen	Die Benutzeroberfläche und Bearbeitungsrechte werden über den Systembenutzer geladen. Datenänderungen werden dem Systembenutzer zugeordnet.

WICHTIG: Standardmäßig ist der Systembenutzer **viadmin** vorhanden. Der Systembenutzer hat die vordefinierte Benutzeroberfläche und die Zugriffsrechte auf Ressourcen der Datenbank. Die Benutzeroberfläche und die Rechtestruktur für den Systembenutzer sollten Sie nicht produktiv nutzen beziehungsweise verändern, da dieser Systembenutzer als Mustersystembenutzer bei jeder Schemaaktualisierung überschrieben wird.

TIPP: Erstellen Sie sich einen eigenen Systembenutzer mit den entsprechenden Berechtigungen. Dies kann bereits bei der initialen Installation der One Identity Manager-Datenbank erfolgen. Diesen Systembenutzer können Sie zum Kompilieren einer initialen One Identity Manager-Datenbank und zur ersten Anmeldung an den Administrationswerkzeugen nutzen.

Single Sign-on generisch (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Anmeldeinformationen	Das Authentifizierungsmodul verwendet die Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • Die Person ist mindestens einer Anwendungsrolle zugewiesen. • Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.
Aktiviert im Standard	nein
Single Sign-on	ja
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Der One Identity Manager sucht laut Konfiguration das Benutzerkonto und ermittelt die Person, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.</p> <p>Datenänderungen werden der angemeldeten Person zugeordnet.</p>

Für den Einsatz des Authentifizierungsmoduls passen Sie im Designer die folgenden Konfigurationsparameter an.

Tabelle 29: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
QER Person GenericAuthenticator	Der Konfigurationsparameter legt fest, ob die Authentifizierung über Single Sign-on unterstützt wird.

Konfigurationsparameter Bedeutung

QER Person GenericAuthenticator SearchTable	Der Konfigurationsparameter enthält die Tabelle im One Identity Manager Schema in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens UID_Person enthalten, der auf die Tabelle Person zeigt. Beispiel: ADSAccount
QER Person GenericAuthenticator SearchColumn	Der Konfigurationsparameter enthält die Spalte aus der One Identity Manager Tabelle (SearchTable), die zur Suche des Benutzernamens des angemeldeten Benutzers verwendet wird. Beispiel: CN
QER Person GenericAuthenticator EnabledBy	Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung aktiviert.
QER Person GenericAuthenticator DisabledBy	Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung deaktiviert. Beispiel: AccountDisabled

Person

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Anmeldeinformationen Zentrales Benutzerkonto und Kennwort der Person.

Voraussetzungen

- Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden.
- Die Person ist in der One Identity Manager-Datenbank vorhanden.
- In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen.
- In den Personenstammdaten ist der Systembenutzer eingetragen.
- In den Personenstammdaten ist das Systembenutzerkennwort eingetragen.

Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der angemeldeten Person direkt zugeordnet ist.</p> <p>Datenänderungen werden der angemeldeten Person zugeordnet.</p>

Person (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Anmeldeinformationen	Zentrales Benutzerkonto und Kennwort der Person.
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen. • In den Personenstammdaten ist das Systembenutzerkennwort eingetragen. • Die Person ist mindestens einer Anwendungsrolle zugewiesen.
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	ja

Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.</p> <p>Datenänderungen werden der angemeldeten Person zugeordnet.</p>

Person (dynamisch)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Anmeldeinformationen	Zentrales Benutzerkonto und Kennwort der Person.
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen. • In den Personenstammdaten ist das Systembenutzerkennwort eingetragen. • Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja

Bemerkungen

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Über die Konfigurationsdaten der Anwendung wird ein Systembenutzer ermittelt und der Person dynamisch zugeordnet. Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der angemeldeten Person dynamisch zugeordnet ist.

Datenänderungen werden der angemeldeten Person zugeordnet.

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109

Benutzerkonto

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Anmeldeinformationen Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.

Voraussetzungen

- Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden.
- Die Person ist in der One Identity Manager-Datenbank vorhanden.
- In den Personenstammdaten sind die zulässigen Anmeldungen eingetragen. Die Anmeldungen werden in der Form: Domäne\Benutzer erwartet.
- In den Personenstammdaten ist der Systembenutzer eingetragen.

Aktiviert im Standard nein

Single Sign-on ja

Anmeldung am ja

Frontend möglich

Anmeldung am Web Portal möglich ja

Bemerkungen Es werden die in der One Identity Manager-Datenbank hinterlegten Anmeldungen aller Personen ermittelt. Zur Anmeldung wird die Person verwendet, deren eingetragene Anmeldung mit den Anmeldeinformationen des angemeldeten Benutzers übereinstimmt.

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der ermittelten Person direkt zugeordnet ist.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Benutzerkonto (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Anmeldeinformationen Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.

Voraussetzungen

- Die Person ist in der One Identity Manager-Datenbank vorhanden.
- In den Personenstammdaten sind die zulässigen Anmeldungen eingetragen. Die Anmeldungen werden in der Form: Domäne\Benutzer erwartet.
- Die Person ist mindestens einer Anwendungsrolle zugewiesen.

Aktiviert im Standard nein

Single Sign-on ja

Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Es werden die in der One Identity Manager-Datenbank hinterlegten Anmeldungen aller Personen ermittelt. Zur Anmeldung wird die Person verwendet, deren eingetragene Anmeldung mit den Anmeldeinformationen des angemeldeten Benutzers übereinstimmt.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.</p> <p>Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.</p>

Kontobasierter Systembenutzer

Anmeldeinformationen	Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.
Voraussetzungen	<ul style="list-style-type: none"> • Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden. • In den Stammdaten des Systembenutzers sind die zulässigen Anmeldungen eingetragen. Die Anmeldungen werden in der Form: Domäne\Benutzer erwartet.
Aktiviert im Standard	nein
Single Sign-on	ja
Anmeldung am Frontend möglich	ja
Anmeldung am Web	nein

Portal möglich

Bemerkungen

Es werden die in der One Identity Manager-Datenbank hinterlegten Anmeldungen aller Systembenutzer ermittelt. Zur Anmeldung wird der Systembenutzer verwendet, deren eingetragene Anmeldung mit den Anmeldeinformationen des angemeldeten Benutzers übereinstimmt.

Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Active Directory Benutzerkonto

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

Anmeldeinformationen Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.

Voraussetzungen

- Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden.
- Die Person ist in der One Identity Manager-Datenbank vorhanden.
- In den Personenstammdaten ist der Systembenutzer eingetragen.
- Das Active Directory Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.

Aktiviert im Standard ja

Single Sign-on ja

Anmeldung am Frontend möglich ja

Anmeldung am Web Portal möglich ja

Bemerkungen

Bei der Anmeldung wird über die SID des Benutzers und die Domäne das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Der One Identity Manager ermittelt die Person, die dem Benutzerkonto zugeordnet ist. Besitzt eine Person mehrere Identitäten, wird über den

Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der ermittelten Person direkt zugeordnet ist. Ist der Person kein Systembenutzer zugeordnet, wird der Systembenutzer aus dem Konfigurationsparameter **SysConfig | Logon | DefaultUser** ermittelt.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

HINWEIS: Wenn Sie bei der Anmeldung im Verbindungsdialog zusätzlich die Option **automatisch verbinden** setzen, so ist bei jeder weiteren Anmeldung keine erneute Authentifizierung notwendig.

Active Directory Benutzerkonto (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

Anmeldeinformationen	Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.
Voraussetzungen	<ul style="list-style-type: none">• Die Person ist in der One Identity Manager-Datenbank vorhanden.• Die Person ist mindestens einer Anwendungsrolle zugewiesen.• Das Active Directory Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.
Aktiviert im Standard	ja
Single Sign-on	ja
Anmeldung am Frontend möglich	ja

Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Bei der Anmeldung wird über die SID des Benutzers und die Domäne das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Der One Identity Manager ermittelt die Person, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.</p> <p>Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.</p>

HINWEIS: Wenn Sie bei der Anmeldung im Verbindungsdialog zusätzlich die Option **automatisch verbinden** setzen, so ist bei jeder weiteren Anmeldung keine erneute Authentifizierung notwendig.

Active Directory Benutzerkonto (manuelle Eingabe)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

Anmeldeinformationen	Anmeldename und Kennwort zur Anmeldung am Active Directory. Die Angabe der Domäne ist nicht erforderlich.
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • Das Active Directory Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen. • Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter TargetSystem ADS Authen-

AuthenticationDomains eingetragen.

- Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.

Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Es werden in der One Identity Manager-Datenbank das entsprechende Benutzerkonto und die Person ermittelt, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none">• Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.• Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Über die Konfigurationsdaten der Anwendung wird ein Systembenutzer ermittelt und der Person dynamisch zugeordnet. Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der angemeldeten Person dynamisch zugeordnet ist.</p> <p>Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.</p>

Active Directory Benutzerkonto (manuelle Eingabe/rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

Anmeldeinformationen	Anmeldename und Kennwort zur Anmeldung am Active Directory. Die Angabe der Domäne ist nicht erforderlich.
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • Die Person ist mindestens einer Anwendungsrolle zugewiesen. • Das Active Directory Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen. • Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter TargetSystem ADS AuthenticationDomains eingetragen.
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Es werden in der One Identity Manager-Datenbank das entsprechende Benutzerkonto und die Person ermittelt, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.</p> <p>Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.</p>

Active Directory Benutzerkonto (dynamisch)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.

Anmeldeinformationen	Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzers.
Voraussetzungen	<ul style="list-style-type: none">• Die Person ist in der One Identity Manager-Datenbank vorhanden.• Das Active Directory Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.• Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.
Aktiviert im Standard	nein
Single Sign-on	ja
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Bei der Anmeldung wird über die SID des Benutzers und die Domäne das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Der One Identity Manager ermittelt die Person, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none">• Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.• Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Über die Konfigurationsdaten der Anwendung wird ein Systembenutzer ermittelt und der Person dynamisch zugeordnet. Die Benutzeroberfläche und die Bearbeitungsrechte</p>

werden über den Systembenutzer geladen, der der angemeldeten Person dynamisch zugeordnet ist.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

HINWEIS: Wenn Sie bei der Anmeldung im Verbindungsdialog zusätzlich die Option **automatisch verbinden** setzen, so ist bei jeder weiteren Anmeldung keine erneute Authentifizierung notwendig.

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109

LDAP Benutzerkonto (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das LDAP Modul vorhanden ist.

Anmeldeinformationen	Anmeldename, Bezeichnung, definierter Name oder Benutzer-ID eines LDAP Benutzerkontos. Kennwort des LDAP Benutzerkontos.
Voraussetzungen	<ul style="list-style-type: none">• Die Person ist in der One Identity Manager-Datenbank vorhanden.• Die Person ist mindestens einer Anwendungsrolle zugewiesen.• Das LDAP Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.• Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja

Bemerkungen

Bei der Anmeldung über den Anmeldenamen, die Bezeichnung oder die Benutzer-ID wird über die Domäne das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter **TargetSystem | LDAP | Authentication | RootDN** eingetragen. Erfolgt die Anmeldung über den definierten Namen, wird das LDAP Benutzerkonto ermittelt, das diesen definierten Namen verwendet. Der One Identity Manager ermittelt die Person, die dem LDAP Benutzerkonto zugeordnet ist.

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Für den Einsatz des Authentifizierungsmoduls passen Sie im Designer die folgenden Konfigurationsparameter an.

Tabelle 30: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
TargetSystem LDAP Authentication	Der Konfigurationsparameter erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem LDAP Authentication Authentication	Der Konfigurationsparameter legt den Authentifizierungsmechanismus fest. Gültige Werte sind Secure, Encryption, SecureSocketsLayer, ReadonlyServer, Anonymous, FastBind, Signing, Sealing, Delegation und ServerBind . Die Werte können mit Komma (,) kombiniert werden. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library . Standard ist ServerBind .
TargetSystem LDAP Authentication Port	Port des LDAP Servers. Standard ist Port 389 .

Konfigurationsparameter Bedeutung

TargetSystem LDAP Authentication RootDN	<p>Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.</p> <p>Syntax:</p> <pre>DC=<MyDomain> DC=<MyOtherDomain></pre> <p>Beispiel:</p> <pre>DC=Root1,DC=com DC=Root2,DC=de</pre>
TargetSystem LDAP Authentication Server	<p>Der Konfigurationsparameter enthält den Namen des LDAP Servers.</p>

LDAP Benutzerkonto (dynamisch)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das LDAP Modul vorhanden ist.

Anmeldeinformationen	<p>Anmeldename, Bezeichnung, definierter Name oder Benutzer-ID eines LDAP Benutzerkontos.</p> <p>Kennwort des LDAP Benutzerkontos.</p>
Voraussetzungen	<ul style="list-style-type: none">• Die Person ist in der One Identity Manager-Datenbank vorhanden.• Das LDAP Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.• Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	Bei der Anmeldung über den Anmeldenamen, die Bezeichnung oder die Benutzer-ID wird über die Domäne das entsprechende

Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter **TargetSystem | LDAP | Authentication | RootDN** eingetragen. Erfolgt die Anmeldung über den definierten Namen, wird das LDAP Benutzerkonto ermittelt, das diesen definierten Namen verwendet. Der One Identity Manager ermittelt die Person, die dem LDAP Benutzerkonto zugeordnet ist.

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Über die Konfigurationsdaten der Anwendung wird ein Systembenutzer ermittelt und der Person dynamisch zugeordnet. Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der angemeldeten Person dynamisch zugeordnet ist.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Für den Einsatz des Authentifizierungsmoduls passen Sie im Designer die folgenden Konfigurationsparameter an.

Tabelle 31: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
TargetSystem LDAP Authentication	Der Konfigurationsparameter erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem LDAP Authentication Authentication	Der Konfigurationsparameter legt den Authentifizierungsmechanismus fest. Gültige Werte sind Secure, Encryption, SecureSocketsLayer, ReadonlyServer, Anonymous, FastBind, Signing, Sealing, Delegation und ServerBind . Die Werte können mit Komma (,) kombiniert werden. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library . Standard ist ServerBind .
TargetSystem LDAP Authentication Port	Port des LDAP Servers. Standard ist Port 389 .
TargetSystem LDAP	Der Konfigurationsparameter enthält eine durch Pipe ()

Konfigurationsparameter Bedeutung

Authentication RootDN	getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll. Syntax: <code>DC=<MyDomain> DC=<MyOtherDomain></code> Beispiel: <code>DC=Root1,DC=com DC=Root2,DC=de</code>
TargetSystem LDAP Authentication Server	Der Konfigurationsparameter enthält den Namen des LDAP Servers.

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109

HTTP Header

Das Authentifizierungsmodul unterstützt die Authentifizierung über Web Single Sign-on Lösungen, die mit einer Proxy-basierten Architektur arbeiten.

Anmeldeinformationen	Zentrales Benutzerkonto oder Personalnummer der Person.
Voraussetzungen	<ul style="list-style-type: none">• Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden.• Die Person ist in der One Identity Manager-Datenbank vorhanden.• In den Personenstammdaten ist das zentrale Benutzerkonto oder die Personalnummer eingetragen.• In den Personenstammdaten ist der Systembenutzer eingetragen.
Aktiviert im Standard	nein
Single Sign-on	ja
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	ja
Bemerkungen	Im HTTP Header muss der Benutzername (in der Form: <code>username = <Benutzername des authentifizierten Benutzers></code>) übergeben werden. In der One Identity Manager-Datenbank wird die Person

ermittelt, deren zentrales Benutzerkonto oder Personalnummer mit dem übergebenen Benutzernamen übereinstimmt.

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der angemeldeten Person direkt zugeordnet ist. Ist der Person kein Systembenutzer zugeordnet, wird der Systembenutzer aus dem Konfigurationsparameter **SysConfig | Logon | DefaultUser** ermittelt.

Datenänderungen werden der angemeldeten Person zugeordnet.

HTTP Header (rollenbasiert)

Das Authentifizierungsmodul unterstützt die Authentifizierung über Web Single Sign-on Lösungen, die mit einer Proxy basierten Architektur arbeiten.

Anmeldeinformationen	Zentrales Benutzerkonto oder Personalnummer der Person.
Voraussetzungen	<ul style="list-style-type: none">• Die Person ist in der One Identity Manager-Datenbank vorhanden.• In den Personenstammdaten ist das zentrale Benutzerkonto oder die Personalnummer eingetragen.• Die Person ist mindestens einer Anwendungsrolle zugewiesen.
Aktiviert im Standard	ja
Single Sign-on	ja
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	ja
Bemerkungen	Im HTTP Header muss der Benutzername (in der Form: <code>username = <Benutzername des authentifizierten Benutzers></code>) übergeben werden. In der One Identity Manager-Datenbank wird die Person

ermittelt, deren zentrales Benutzerkonto oder Personalnummer mit dem übergebenen Benutzernamen übereinstimmt.

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.

Datenänderungen werden der angemeldeten Person zugeordnet.

OAuth 2.0/OpenID Connect

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Das Authentifizierungsmodul unterstützt den Autorisierungscodefluss für OAuth 2.0 und OpenID Connect. Detaillierte Informationen zum Autorisierungscodefluss erhalten Sie beispielsweise in der [OAuth Spezifikation](#) oder der [OpenID Connect Spezifikation](#).

Das Authentifizierungsmodul verwendet einen Sicherheitstokendienst (Secure Token Service) zur Anmeldung. Dieses Anmeldeverfahren kann mit jedem Sicherheitstokendienst eingesetzt werden, der OAuth 2.0 Token zurückgeben kann.

Anmeldeinformationen	Abhängig vom Authentifizierungsverfahren des Sicherheitstokendienstes.
Voraussetzungen	<ul style="list-style-type: none">• Der Systembenutzer mit Berechtigungen ist in der One Identity Manager-Datenbank vorhanden.• Die Person ist in der One Identity Manager-Datenbank vorhanden.• In den Personenstammdaten ist der Systembenutzer eingetragen.• Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.
Aktiviert im Standard	nein

Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Der One Identity Manager ermittelt die Person, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Die Benutzeroberfläche und Bearbeitungsrechte werden über den Systembenutzer geladen, der der ermittelten Person direkt zugeordnet ist.</p> <p>Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet. Dafür muss der Claim-Typ bekannt sein, dessen Wert zur Kennzeichnung der Datenänderungen verwendet wird.</p>

Verwandte Themen

- [OAuth 2.0/OpenID Connect Konfiguration](#) auf Seite 115
- [Ablauf der OAuth 2.0/OpenID Connect Authentifizierung](#) auf Seite 115

OAuth 2.0/OpenID Connect (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Das Authentifizierungsmodul unterstützt den Autorisierungscodefluss für OAuth 2.0 und OpenID Connect. Detaillierte Informationen zum Autorisierungscodefluss erhalten Sie beispielsweise in der [OAuth Spezifikation](#) oder der [OpenID Connect Spezifikation](#).

Das Authentifizierungsmodul verwendet einen Sicherheitstokendienst (Secure Token Service) zur Anmeldung. Dieses Anmeldeverfahren kann mit jedem Sicherheitstokendienst eingesetzt werden, der OAuth 2.0 Token zurückgeben kann.

Anmeldeinformationen	Abhängig vom Authentifizierungsverfahren des Sicherheitstokendienstes.
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • Die Person ist mindestens einer Anwendungsrolle zugewiesen. • Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	<p>Der One Identity Manager ermittelt die Person, die dem Benutzerkonto zugeordnet ist.</p> <p>Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter QER Person MasterIdentity UseMasterForAuthentication gesteuert, welche Person zur Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. <p>Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.</p> <p>Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet. Dafür muss der Claim-Typ bekannt sein, dessen Wert zur Kennzeichnung der Datenänderungen verwendet wird.</p>

Verwandte Themen

- [OAuth 2.0/OpenID Connect Konfiguration](#) auf Seite 115
- [Ablauf der OAuth 2.0/OpenID Connect Authentifizierung](#) auf Seite 115

Synchronisationsauthenticator

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Modul Zielsystemsynchronisation vorhanden ist.

Das Authentifizierungsmodul integriert das Standardverfahren zur Anmeldung des Synchronization Editor.

Anmeldeinformationen	Die Anmeldung erfolgt über den Systembenutzer sa .
Voraussetzungen	
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	Den Systembenutzer sa sollten Sie nicht verändern. Der Systembenutzer wird bei jeder Schemaaktualisierung überschrieben.

Web Agent Authenticator

Das Authentifizierungsmodul integriert das Standardverfahren zur Anmeldung des Web Designer, um vor der ersten Benutzeranmeldung auf die Datenbank zuzugreifen.

Anmeldeinformationen	Die Anmeldung erfolgt über den Systembenutzer sa .
Voraussetzungen	
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	Den Systembenutzer sa sollten Sie nicht verändern. Der Systembenutzer wird bei jeder Schemaaktualisierung überschrieben.

Component Authenticator

Das Authentifizierungsmodul integriert das Standardverfahren zur Anmeldung der Prozesskomponenten.

Anmeldeinformationen	Die Anmeldung erfolgt über den Systembenutzer sa .
Voraussetzungen	
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	Den Systembenutzer sa sollten Sie nicht verändern. Der Systembenutzer wird bei jeder Schemaaktualisierung überschrieben.

Crawler

Das Authentifizierungsmodul wird vom Anwendungsserver zum Aufbau des Suchindexes für die Volltextsuche über die Datenbank verwendet.

Anmeldeinformationen	Die Anmeldung erfolgt über den Systembenutzer sa .
Voraussetzungen	
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	Den Systembenutzer sa sollten Sie nicht verändern. Der Systembenutzer wird bei jeder Schemaaktualisierung überschrieben.

Kennworrücksetzung

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Das Authentifizierungsmodul wird zur Anmeldung am Kennworrücksetzungsportal verwendet. Das Authentifizierungsmodul prüft den Zugangscode oder die Antworten auf die Kennwortabfragen der Person. Erfolgt die Anmeldung über den Zugangscode wird dieser nach erfolgreicher Anmeldung gelöscht.

Anmeldeinformationen	Zentrales Benutzerkonto und Zugangscode. - ODER - Zentrales Benutzerkonto und Antworten auf die Kennwortabfragen. - ODER - Zielsystembenutzerkonto und Zugangscode. - ODER - Zielsystembenutzerkonto und Antworten auf die Kennwortabfragen.
Voraussetzungen	<ul style="list-style-type: none">• Die Person ist in der One Identity Manager-Datenbank vorhanden.• Bei Verwendung des zentralen Benutzerkontos: In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen.• Bei Verwendung des Zielsystembenutzerkontos: Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen.• Die Person ist nicht deaktiviert oder hat den Zertifizierungsstatus Neu.• Die Person hat einen Zugangscode oder die Fragen und Antworten zur Kennwortabfrage sind hinterlegt.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	Das Anwendungstoken für das Kennworrücksetzungsportal muss eingetragen sein. Das Anwendungstoken setzen Sie bei der Installation des Kennworrücksetzungsportals. Das

Anwendungstoken wird in der Datenbank im Konfigurationsparameter **QER | Person | PasswordResetAuthenticator | ApplicationToken** als Hashwert gespeichert und in der Datei `web.config` der Webanwendung verschlüsselt abgelegt. Ausführliche Informationen zur Einrichtung des Kennworrücksetzungsportals finden Sie im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Für die Verwendung eines Zielsystembenutzerkontos zur Anmeldung passen Sie im Designer die folgenden Konfigurationsparameter an. Sind die Konfigurationsparameter nicht aktiviert, wird das zentrale Benutzerkonto der Person zur Anmeldung verwendet.

Tabelle 32: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
QER Person PasswordResetAuthenticator SearchTable	Der Konfigurationsparameter enthält die Tabelle im One Identity Manager Schema in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens <code>UID_Person</code> enthalten, der auf die Tabelle <code>Person</code> zeigt. Beispiel: <code>ADSAccount</code>
QER Person PasswordResetAuthenticator SearchColumn	Der Konfigurationsparameter enthält die Spalte aus der One Identity Manager Tabelle (SearchTable), die zur Suche des Benutzernamens des angemeldeten Benutzers verwendet wird. Beispiel: <code>CN</code>
QER Person PasswordResetAuthenticator EnabledBy	Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung aktiviert.
QER Person PasswordResetAuthenticator DisabledBy	Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung deaktiviert. Beispiel: <code>AccountDisabled</code>

Kennworrücksetzung (rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul vorhanden ist.

Das Authentifizierungsmodul wird zur Anmeldung am Kennworrücksetzungsportal verwendet. Das Authentifizierungsmodul prüft den Zugangscode oder die Antworten auf die Kennwortabfragen der Person. Erfolgt die Anmeldung über den Zugangscode wird dieser nach erfolgreicher Anmeldung gelöscht.

Anmeldeinformationen	<p>Zentrales Benutzerkonto und Zugangscode.</p> <p>- ODER -</p> <p>Zentrales Benutzerkonto und Antworten auf die Kennwortabfragen.</p> <p>- ODER -</p> <p>Zielsystembenutzerkonto und Zugangscode.</p> <p>- ODER -</p> <p>Zielsystembenutzerkonto und Antworten auf die Kennwortabfragen.</p>
Voraussetzungen	<ul style="list-style-type: none"> • Die Person ist in der One Identity Manager-Datenbank vorhanden. • Bei Verwendung des zentralen Benutzerkontos: In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen. • Bei Verwendung des Zielsystembenutzerkontos: Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen. • Die Person ist nicht deaktiviert oder hat den Zertifizierungsstatus Neu. • Die Person hat einen Zugangscode oder die Fragen und Antworten zur Kennwortabfrage sind hinterlegt. • Die Person ist mindestens einer Anwendungsrolle zugewiesen.
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	<p>Das Anwendungstoken für das Kennworrücksetzungsportal muss eingetragen sein. Das Anwendungstoken setzen Sie bei der Installation des Kennworrücksetzungsportals. Das Anwendungstoken wird in der Datenbank im Konfigurationsparameter QER Person PasswordResetAuthenticator ApplicationToken als Hashwert gespeichert und in der Datei <code>web.config</code> der</p>

Webanwendung verschlüsselt abgelegt. Ausführliche Informationen zur Einrichtung des Kennwortrücksetzungsportals finden Sie im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.

Für die Verwendung eines Zielsystembenutzerkontos zur Anmeldung passen Sie im Designer die folgenden Konfigurationsparameter an. Sind die Konfigurationsparameter nicht aktiviert, wird das zentrale Benutzerkonto der Person zur Anmeldung verwendet.

Tabelle 33: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
QER Person PasswordResetAuthenticator SearchTable	Der Konfigurationsparameter enthält die Tabelle im One Identity Manager Schema in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens UID_Person enthalten, der auf die Tabelle Person zeigt. Beispiel: ADSAccount
QER Person PasswordResetAuthenticator SearchColumn	Der Konfigurationsparameter enthält die Spalte aus der One Identity Manager Tabelle (SearchTable), die zur Suche des Benutzernamens des angemeldeten Benutzers verwendet wird. Beispiel: CN
QER Person PasswordResetAuthenticator EnabledBy	Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung aktiviert.
QER Person PasswordResetAuthenticator DisabledBy	Der Konfigurationsparameter enthält eine durch Pipe () getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung deaktiviert. Beispiel: AccountDisabled

Bearbeiten der Authentifizierungsmodule

Um ein Authentifizierungsmodul zur Anmeldung zu verwenden, sind folgende Voraussetzungen zu erfüllen:

1. Das Authentifizierungsmodul muss aktiviert sein.
2. Das Authentifizierungsmodul muss der Anwendung zugewiesen sein.
3. Die Zuweisung des Authentifizierungsmoduls zur Anwendung muss aktiviert sein.

Damit ist die Anmeldung mit diesem Authentifizierungsmodul an den zugewiesenen Anwendungen möglich. Stellen Sie sicher, dass die Benutzer, die durch das Authentifizierungsmodul ermittelt werden, auch die benötigten Programmfunktionen besitzen, die Anwendung zu benutzen.

Detaillierte Informationen zum Thema

- [Authentifizierungsmodule aktivieren](#) auf Seite 102
- [Authentifizierungsmodule zu Anwendungen zuweisen](#) auf Seite 103
- [Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren](#) auf Seite 103
- [Eigenschaften von Authentifizierungsmodulen](#) auf Seite 104
- [Initiale Daten für Authentifizierungsmodule](#) auf Seite 105
- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109
- [One Identity Manager Authentifizierungsmodule](#) auf Seite 72
- [Steuern von Berechtigungen über Programmfunktionen](#) auf Seite 64

Authentifizierungsmodule aktivieren

Um ein Authentifizierungsmodul zu aktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Authentifizierungsmodule**.
2. Wählen Sie im Listeneditor das Authentifizierungsmodul.
3. Setzen Sie in der Ansicht **Eigenschaften** die Eigenschaft **Aktiviert** auf den Wert **True**.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren](#) auf Seite 103

Authentifizierungsmodule zu Anwendungen zuweisen

Wenn Sie kundenspezifische Authentifizierungsmodule entwickeln, weisen Sie diese den vorhandenen Anwendungen zu. Zuweisungen vordefinierter Authentifizierungsmodule müssen Sie in der Regel nicht ändern.

HINWEIS: Für die Anmeldung am Designer verwenden Sie nicht-rollenbasierte Authentifizierungsmodule. Rollenbasierte Authentifizierungsmodule werden für die Anmeldung am Designer nicht unterstützt.

Um ein Authentifizierungsmodul an Anwendungen zuzuordnen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Authentifizierungsmodule**.
2. Wählen Sie den Menüeintrag **Ansicht | Tabellenrelationen wählen** und aktivieren Sie die Tabelle `DialogProductHasAuthentifizier`.
3. Wählen Sie im Listeneditor das Authentifizierungsmodul.
4. Weisen Sie in der Bearbeitungsansicht **Anwendung** die Anwendung zu.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren](#) auf Seite 103

Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren

Um ein Authentifizierungsmodul für eine Anwendung zu deaktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Anwendungen**.
2. Wählen Sie im Listeneditor die Anwendung und wählen Sie die Aufgabe **Überblick zur Anwendung**.
3. Wählen Sie im Formularelement **Wirksame Authentifizierungsmodule** das Authentifizierungsmodul.

4. Starten Sie den Objekteditor über die Aufgabe **Objekt bearbeiten**.
5. Ändern Sie in der Eigenschaft **Deaktiviert** den Wert auf **True**.
6. Speichern Sie die Änderungen.

Um ein Authentifizierungsmodul für eine Anwendung zu aktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Anwendungen**.
2. Wählen Sie im Listeneditor die Anwendung und wählen Sie die Aufgabe **Überblick zur Anwendung**.
3. Wählen Sie im Formularelement **Deaktivierte Authentifizierungsmodule** das Authentifizierungsmodul.
4. Starten Sie den Objekteditor über die Aufgabe **Objekt bearbeiten**.
5. Ändern Sie in der Eigenschaft **Deaktiviert** den Wert auf **False**.
6. Speichern Sie die Änderungen.

Verwandte Themen

- [Authentifizierungsmodule zu Anwendungen zuweisen](#) auf Seite 103
- [Authentifizierungsmodule aktivieren](#) auf Seite 102

Eigenschaften von Authentifizierungsmodulen

Tabelle 34: Eigenschaften von Authentifizierungsmodulen

Eigenschaft	Bedeutung
Aktiviert	Angabe, ob das Authentifizierungsmoduls zur Verwendung aktiviert ist.
Anzeigename	Der Anzeigename wird zur Anzeige des Authentifizierungsmoduls im Anmeldedialog der Administrationswerkzeuge verwendet.
Authentifizierungsmodul	Interner Name des Authentifizierungsmoduls.
Authentifizierungstyp	Legt den Typ des Authentifizierungsmoduls fest. Zur Auswahl stehen Dynamisch und Rollenbasiert .
Bearbeitungsstatus	Der Bearbeitungsstatus wird bei der Erstellung von Kundenkonfigurationspaketen genutzt.
Initiale Daten	Initiale Daten für die Anmeldung mit diesem Authentifizierungsmodul.

Eigenschaft	Bedeutung
Klasse	Klasse des Authentifizierungsmoduls.
Name des Assemblies	Name des Assemblies.
Reihenfolge	Reihenfolge für die Anzeige im Anmeldedialog.
Single Sign On	Angabe, ob das Authentifizierungsmodul ohne Angabe eines Kennwortes authentifizieren darf.
Wählbar im Frontend	Angabe, ob das Authentifizierungsmodul im Anmeldedialog zur Auswahl angeboten werden soll.

Initiale Daten für Authentifizierungsmodule

Die initialen Daten sind ein Teil des Authentication-Strings (Parameter-/Wert-Paare ohne Modulkennung). Initiale Daten aus dem Authentication-String, werden bei jedem Authentifizierungsvorgang als Standard vorbelegt.

Der Authentication-String ist nach folgendem Muster aufgebaut:

Module=<Name>;<Property1>=<Wert1>;<Property2>=<Wert2>,...

Beispiel:

Module=DialogUser;User=<user name>;Password=<password>

Um initiale Daten festzulegen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Authentifizierungsmodule**.
2. Wählen Sie das Authentifizierungsmodul und geben Sie im Eingabefeld **Initiale Daten** die Daten ein.

Syntax:

Property1=Wert1;Property2=Wert2

Beispiel:

User=<user name>;Password=<password>

Abhängig vom Authentifizierungsmodul können verschiedene initiale Daten verwendet werden.

Tabelle 35: Initiale Daten für Authentifizierungsmodule

Anzeigename des Moduls	Authentifizierungsmodul	Parameter	Bedeutung/Anmerkung
Systembenutzer	DialogUser	User	Benutzername.
		Password	Kennwort des Benutzers.

Anzeigename des Moduls	Authentifizierungsmodul	Parameter	Bedeutung/ Anmerkung
Active Directory Benutzerkonto	ADSAccount		
Active Directory Benutzerkonto (dynamisch)	DynamicADSAccount	Product	Anwendung. Der Systembenutzer wird über die Konfigurationsdaten der Anwendung bestimmt.
Active Directory Benutzerkonto (manuelle Eingabe)	DynamicManualADS	Product	Anwendung. Der Systembenutzer wird über die Konfigurationsdaten der Anwendung bestimmt.
		User	Benutzername. Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Die zulässigen Active Directory Domänen geben Sie im Konfigurationsparameter TargetSystem ADS AuthenticationDomains an.
		Password	Kennwort des Benutzers.
Active Directory Benutzerkonto (rollenbasiert)	RoleBasedADSAccount		Keine Parameter erforderlich.
Active Directory Benutzerkonto (manuelle Eingabe/rollenbasiert)	RoleBasedManualADS	User	Benutzername. Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Die zulässigen Active Directory Domänen geben Sie im Konfigurationsparameter TargetSystem ADS AuthenticationDomains an.

Anzeigename des Moduls	Authentifizierungsmodul	Parameter	Bedeutung/ Anmerkung
		Password	Kennwort des Benutzers.
Person	Person	User	Zentrales Benutzerkonto der Person.
		Password	Kennwort des Benutzers.
Person (dynamisch)	DynamicPerson	Product	Anwendung. Der Systembenutzer wird über die Konfigurationsdaten der Anwendung bestimmt.
		User	Benutzername.
		Password	Kennwort des Benutzers.
Person (rollenbasiert)	RoleBasedPerson	User	Benutzername.
		Password	Kennwort des Benutzers.
HTTP Header	HTTPHeader	Header	Zu nutzender HTTP Header.
		KeyColumn	Kommagetrennte Liste der Spalten in der Tabelle Person, in denen nach dem Benutzernamen gesucht werden soll. Standard: CentralAccount, PersonnelNumber
HTTP Header (rollenbasiert)	RoleBasedHTTPHeader		Zu nutzender HTTP-Header.
		KeyColumn	Kommagetrennte Liste der Spalten in Tabelle Person, in denen nach dem Benutzernamen gesucht werden soll. Standard: CentralAccount, PersonnelNumber
LDAP Benutzerkonto (dynamisch)	DynamicLdap	User	Benutzername. Standard: CN,

Anzeigename des Moduls	Authentifizierungsmodul	Parameter	Bedeutung/ Anmerkung
			DistinguishedName, UserID, UIDLDAP
		Password	Kennwort des Benutzers.
LDAP Benutzerkonto (rollenbasiert)	RoleBasedLdap	User	Benutzername. Standard: CN, DistinguishedName, UserID, UIDLDAP
		Password	Kennwort des Benutzers.
Single Sign-on generisch (rollenbasiert)	RoleBasedGeneric	SearchTable	Tabelle, in welcher nach dem Benutzernamen des angemeldeten Benutzers gesucht wird. Diese Tabelle muss einen FK namens UID_Person enthalten, der auf die Tabelle Person zeigt.
		SearchColumn	Spalte aus der SearchTable, in welcher nach dem Benutzernamen des angemeldeten Benutzers gesucht wird.
		DisabledBy	Durch Pipe () getrennte Liste von booleschen Spalten, welche ein Benutzerkonto für das Anmelden sperren.
		EnabledBy	Durch Pipe () getrennte Liste von booleschen Spalten, welche ein Benutzerkonto für das Anmelden freischalten.
OAuth 2.0/OpenID Connect	OAuth		Abhängig vom Authentifizierungsverfahren des Sicherheitstokendienstes.
OAuth 2.0/OpenID Connect (rollenbasiert)	OAuthRoleBased		Abhängig vom Authentifizierungsverfahren des Sicher-

Anzeigename des Moduls	Authentifizierungsmodul	Parameter	Bedeutung/Anmerkung
			heitstokendienstes.
Kontobasierter Systembenutzer	DialogUserAccountBased		Keine Parameter erforderlich.
Benutzerkonto	QERAccount		Keine Parameter erforderlich.
Benutzerkonto (rollenbasiert)	RoleBasedQERAccount		Keine Parameter erforderlich.
Kennwort-rücksetzung	PasswordReset		Keine Parameter erforderlich.
Kennwort-rücksetzung (rollenbasiert)	RoleBasedPasswordReset		Keine Parameter erforderlich.

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109
- [One Identity Manager Authentifizierungsmodule](#) auf Seite 72

Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers

Bei den dynamischen Authentifizierungsmodulen wird nicht der an einer Person direkt eingetragene Systembenutzer zur Anmeldung genutzt, sondern der anzuwendende Systembenutzer über spezielle Konfigurationsdaten der Benutzeroberfläche bestimmt.

Um Konfigurationsdaten festzulegen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Anwendungen**.
2. Wählen Sie die Anwendung und passen Sie die **Konfigurationsdaten** an.

Die Konfigurationsdaten erfassen Sie in XML-Syntax:

```
<DialogUserDetect>
  <Usermappings>
    <Usermapping
      DialogUser = "Name des Systembenutzers"
```

```

        Selection = "Auswahlkriterium"
    />
    <Usermapping
        DialogUser = "Name des Systembenutzers"
    />
    ...
</Usermappings>
</DialogUserDetect>

```

In der Sektion Usermappings geben Sie die Systembenutzer (DialogUser) an. Über ein Auswahlkriterium (Selection) legen Sie fest, welche Personen den angegebenen Systembenutzer verwenden sollen. Die Angabe eines Auswahlkriteriums für die Zuordnung ist nicht zwingend erforderlich. Es wird der Systembenutzer aus der ersten zutreffenden Zuordnung zur Anmeldung verwendet.

Für eine komplexe Rechte- und Benutzeroberflächenstruktur können Sie eine Zuordnung von Funktionsgruppen zu Rechtegruppen vornehmen. Über Funktionsgruppen bilden Sie die Funktionen der Personen in einem Unternehmen ab, beispielsweise IT Controller oder Niederlassungsleiter. Die Funktionsgruppen ordnen Sie den Rechtegruppen zu. Eine Funktionsgruppe kann auf mehrere Rechtegruppen verweisen und es können mehrere Funktionsgruppen auf eine Rechtegruppe verweisen.

Ist die Sektion FunctionGroupMapping in den Konfigurationsdaten enthalten, so wird diese zuerst ausgewertet und der ermittelte Systembenutzer verwendet. Das Authentifizierungsmodul verwendet den Systembenutzer zur Anmeldung, der genau in den ermittelten Rechtegruppen Mitglied ist. Wird so kein Systembenutzer ermittelt, wird die Sektion Usermapping ausgewertet.

```

<DialogUserDetect>
    <FunctionGroupMapping
        PersonToFunction = "View Mapping Person auf Funktionsgruppe"
        FunctionToGroup = "View Mapping Funktionsgruppe auf Rechtegruppe"
    />
    <Usermappings>
        <Usermapping
            DialogUser = "Name des Systembenutzers"
            Selection = "Auswahlkriterium"
        />
        ...
    </Usermappings>
</DialogUserDetect>

```

Verwandte Themen

- [Beispiel für eine einfache Zuordnung zum Systembenutzer](#) auf Seite 111
- [Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium](#) auf Seite 112
- [Beispiel für eine Zuordnung über Funktionsgruppen](#) auf Seite 113
- [Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen](#) auf Seite 36

Beispiel für eine einfache Zuordnung zum Systembenutzer

In einem Webfrontend soll die Benutzeroberfläche für den IT Shop für alle Personen, ohne Berücksichtigung von Rechten auf Tabellen und Spalten angezeigt werden.

Dazu richten Sie eine neue Anwendung ein, beispielsweise **WebShop_Customer_Prd**, und passen die Konfigurationsdaten wie folgt an:

```
<DialogUserDetect>
  <Usermappings>
    <Usermapping
      DialogUser = "dlg_all"
    />
  </Usermappings>
</DialogUserDetect>
```

Legen Sie eine neue Rechtegruppe **WebShop_Customer_Grp** an, welche die Benutzeroberfläche für die Anwendung, bestehend aus den Menüeinträgen, Oberflächenformularen und Methodendefinitionen, erhält. Die Benutzeroberfläche könnte aus den folgenden Menüeinträgen bestehen:

- Kontaktdaten des Mitarbeiters
- Bestellen eines Artikels
- Abbestellen eines Artikels

Definieren Sie einen neuen Systembenutzer **dlg_all** und nehmen Sie diesen in die Rechtegruppen **vi_DE-CentralPwd**, **vi_DE-ITShopOrder** und **WebShop_Customer_Grp** auf.

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109

- [Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 112](#)
- [Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 113](#)
- [Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen auf Seite 36](#)

Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium

Das im vorhergehenden Beispiel beschriebene Szenario wird so erweitert, dass nur der Kostenstellenverantwortliche das Austrittsdatum eines Mitarbeiters sehen darf. Dazu erweitern Sie das Kontaktdatenformular um das Eingabefeld **Austrittsdatum**.

Die Steuerung der Sichtbarkeit und Bearbeitbarkeit erfolgt über die Rechte. Richten Sie einen neuen Systembenutzer **dlg_kst** ein und nehmen Sie diesen in die Rechtegruppen **vi_DE-CentralPwd**, **vi_DE-ITShopOrder** und **WebShop_Customer_Grp** auf. Dem Systembenutzer geben Sie zusätzlich das Sichtbarkeitsrecht und das Bearbeitungsrecht auf die Spalte `Person.Exitdate`.

Die Konfigurationsdaten der Anwendung erweitern Sie so, dass die Kostenstellenverantwortlichen den Systembenutzer **dlg_kst** zur Anmeldung verwenden. Alle anderen Personen nutzen den Systembenutzer **dlg_all** zur Anmeldung.

Die Konfigurationsdaten passen Sie wie folgt an:

```
<DialogUserDetect>
  <Usermappings>
    <Usermapping
      DialogUser = "dlg_kst"
      Selection = "select 1 where %uid% in (select uid_personhead from profitcenter)"
    />
    <Usermapping
      DialogUser = "dlg_all"
    />
  </Usermappings>
</DialogUserDetect>
```

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 109](#)
- [Beispiel für eine einfache Zuordnung zum Systembenutzer auf Seite 111](#)
- [Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 113](#)

- [Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen auf Seite 36](#)

Beispiel für eine Zuordnung über Funktionsgruppen

Für die Zuordnung von Funktionsgruppen zu Rechtegruppen müssen Sie zwei Datenbanksichten definieren. Die erste Datenbanksicht liefert die Zuordnung der Personen zu Funktionsgruppen. Die Datenbanksicht enthält die zwei Spalten UID_Person und FunctionGroup.

Beispiel:

```
create view custom_Person2Fu as
    select uid_personHead as UID_Person, 'Kostenstellenverantwortliche' as
    FunctionGroup
    from Profitcenter
    where isnull(uid_personHead, '') > ' '
    union all
    select uid_personHead, 'Abteilungsleiter' as FunctionGroup
    from Department
    where isnull(uid_personHead, '') > ' '
```

Die zweite Datenbanksicht nimmt die Zuordnung der Funktionsgruppen zu den Rechtegruppen vor. Diese Datenbanksicht enthält die zwei Spalten FunctionGroup und DialogGroup.

Beispiel:

```
create view custom_Fu2D as
    select 'Kostenstellenverantwortliche' as FunctionGroup, '<UID_Custom_Dialoggroup_
    ChefP>' as DialogGroup
    union all select 'Abteilungsleiter', '<UID_Custom_Dialoggroup_ChefD>' as
    DialogGroup
```

Richten Sie rollenbasierte Rechtegruppen mit den notwendigen Berechtigungen ein.

TIPP: Eine rollenbasierte Rechtegruppe kann von nicht-rollenbasierten Rechtegruppen erben. Somit können Sie eine Vererbungshierarchie aufbauen, um die Berechtigungen einfacher zu vergeben.

Die Konfigurationsdaten zur Zuordnung von Funktionsgruppen zu Rechtegruppen passen Sie wie folgt an:

```
<DialogUserDetect>
    <FunctionGroupMapping
        PersonToFunction = "custom_Person2Fu"
```

```
        FunctionToGroup = "custom_Fu2D"  
    />  
</DialogUserDetect>
```

Verwandte Themen

- [Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers](#) auf Seite 109
- [Beispiel für eine einfache Zuordnung zum Systembenutzer](#) auf Seite 111
- [Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium](#) auf Seite 112
- [Erteilen von Berechtigungen auf das One Identity Manager Schema über Rechtegruppen](#) auf Seite 36

Überprüfung der Authentifizierung

Bei der Anmeldung eines Benutzers erfolgt eine Gültigkeitsprüfung. Über Einstellungen können Sie zusätzlich konfigurieren.

- Um zu verhindern, dass Benutzer mit ihren bestehenden Verbindungen arbeiten, wenn sie seit ihrer Anmeldung deaktiviert wurden, führt das System zusätzliche Gültigkeitsprüfungen im definierten Zeitabstand aus. Die Prüfung erfolgt bei der nächsten rechtebasierten Aktion auf der Verbindung nach einem festgelegten Intervall von 20 Minuten.

Das Intervall können Sie über den Konfigurationsparameter **Common | Authentication | CheckInterval** anpassen. Bearbeiten Sie den Konfigurationsparameter im Designer.

- Die Anzahl der Sitzungen, die ein Benutzer innerhalb kurzer Zeit öffnen darf, ist begrenzt auf 10 Sitzungen in einer Minute.

Ist die Anzahl überschritten, erhält der Benutzer eine Fehlermeldung:

Sie haben sich in der letzten Minute zu häufig angemeldet. Bitte warten Sie einen Moment mit einer Neuansmeldung.

Bei lokaler Anmeldung erfolgt die Prüfung je Frontend. Bei Anmeldung über den Anwendungsserver erfolgt die Prüfung je Anwendungsserver.

Die Anzahl der Sitzungen können Sie über den Konfigurationsparameter **Common | Authentication | SessionsPerUserAndMinute** anpassen. Bearbeiten Sie den Konfigurationsparameter im Designer.

- Legen Sie über den Konfigurationsparameter **QBM | AppServer | SessionTimeout** den Zeitraum in Stunden fest, nach dem nicht mehr benutzte Sitzungen eines Anwendungsserver geschlossen werden. Der Standardwert ist **24** Stunden. Bearbeiten Sie den Konfigurationsparameter im Designer.

OAuth 2.0/OpenID Connect Konfiguration

Die Authentifizierungsmodule **OAuth2.0/OpenID Connect** und **OAuth2.0/OpenID Connect (rollenbasiert)** unterstützen den Autorisierungscodefluss für OAuth 2.0 und OpenID Connect. Detaillierte Informationen zum Autorisierungscodefluss erhalten Sie beispielsweise in der [OAuth Spezifikation](#) oder der [OpenID Connect Spezifikation](#).

Um die OAuth2.0/OpenID Connect Authentifizierung zu nutzen:

- Erstellen Sie im Designer den Identitätsanbieter und die OAuth2.0/OpenID Connect Anwendungen beim Identitätsanbieter. Dazu wird im Designer ein Assistent angeboten.
- Weisen Sie den Webanwendungen die OAuth2.0/OpenID Connect Anwendung zu.

Verwandte Themen

- [Ablauf der OAuth 2.0/OpenID Connect Authentifizierung](#) auf Seite 115
- [OAuth 2.0/OpenID Connect Konfiguration erstellen](#) auf Seite 117
- [OAuth 2.0/OpenID Connect Konfiguration an Webanwendungen zuweisen](#) auf Seite 121
- [Aktivierende und deaktivierende Spalten für die Anmeldung festlegen](#) auf Seite 123
- [OAuth 2.0/OpenID Connect](#) auf Seite 93
- [OAuth 2.0/OpenID Connect \(rollenbasiert\)](#) auf Seite 94
- [Informationen für OAuth 2.0/OpenID Connect Authentifizierung aufzeichnen](#) auf Seite 125

Ablauf der OAuth 2.0/OpenID Connect Authentifizierung

Die Webanwendung (oder native Anwendung) fordert am Authorisierungsendpunkt den Autorisierungscode an. Über den Anmeldeendpunkt wird ein erweiterter Anmeldedialog

aufgerufen, über den der Autorisierungscode ermittelt wird. Das Authentifizierungsmodul fordert ein Zugriffstoken vom Tokenendpunkt an. Zur Prüfung des Sicherheitstokens wird das Zertifikat herangezogen.

Dabei wird zunächst versucht, das Zertifikat aus der Konfiguration der Webanwendung zu ermitteln. Ist dies nicht möglich, werden die Einstellungen des Identitätsanbieters verwendet. Um das Zertifikat zur Prüfung der Token zu ermitteln, werden die Zertifikatsspeicher in folgender Reihenfolge abgefragt:

1. Konfiguration der OAuth 2.0/OpenID Connect Anwendung (Tabelle `QBMIIdentityClient`)
 - a. Zertifikatstext (`QBMIIdentityClient.CertificateText`) .
 - b. Subjekt oder Fingerabdruck aus dem lokalen Speicher (`QBMIIdentityClient.CertificateSubject` und `QBMIIdentityClient.CertificateThumbPrint`).
 - c. Zertifikatsendpunkt (`QBMIIdentityClient.CertificateEndpoint`).
Zusätzlich werden das Subjekt oder der Fingerabdruck verwendet, um Zertifikate vom Server zu prüfen, wenn sie angegeben sind und nicht auf dem Server lokal existieren.
2. Konfiguration des Identitätsanbieters (Tabelle `QBMIIdentityProvider`)
 - a. Zertifikatstext (`QBMIIdentityProvider.CertificateText`).
 - b. Subject oder Fingerabdruck aus dem lokalen Speicher (`QBMIIdentityProvider.CertificateSubject` und `QBMIIdentityProvider.CertificateThumbPrint`).
 - c. Zertifikatsendpunkt (`QBMIIdentityProvider.CertificateEndpoint`)).
Zusätzlich werden das Subjekt oder der Fingerabdruck verwendet, um Zertifikate vom Server zu prüfen, wenn sie angegeben sind und nicht auf dem Server lokal existieren.
 - d. JSON-Web-Key-Endpunkt (`QBMIIdentityProvider.JsonWebKeyEndpoint`).

Um das Benutzerkonto zu ermitteln, wird festgelegt über welchen Claim-Typ die Benutzerinformationen ermittelt werden und welche Informationen des One Identity Manager Schemas zur Suche des Benutzerkontos verwendet werden.

Die Authentifizierung über OpenID Connect baut auf OAuth 2.0 auf. Die OpenID Connect Authentifizierung benutzt dieselben Mechanismen, stellt aber die Benutzer-Claims in einem ID-Token oder über einen UserInfo-Endpunkt zur Verfügung. Für den Einsatz von OpenID Connect sind weitere Konfigurationseinstellungen erforderlich. Ist im **Scope** der Wert **openid** enthalten, verwenden die Authentifizierungsmodule OpenID Connect zur Authentifizierung.

Verwandte Themen

- [OAuth 2.0/OpenID Connect Konfiguration erstellen](#) auf Seite 117
- [OAuth 2.0/OpenID Connect](#) auf Seite 93
- [OAuth 2.0/OpenID Connect \(rollenbasiert\)](#) auf Seite 94

OAuth 2.0/OpenID Connect Konfiguration erstellen

Um eine OAuth 2.0/OpenID Connect Konfiguration zu erstellen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | OAuth 2.0/OpenID Connect Konfiguration**.
2. Wählen Sie die Aufgabe **Einen neuen Identitätsanbieter erstellen**.
3. Auf der Startseite des Assistenten klicken Sie **Weiter**.
4. Auf der Seite **Neuer Identitätsanbieter** erfassen Sie den Anzeigenamen der Konfiguration und eine Beschreibung.
5. Klicken Sie **Weiter**.
6. Auf der Seite **Automatische Konfigurationsermittlung** legen Sie fest, wie Sie die Informationen zum Identitätsanbieter eingeben möchten.
 - Wenn die Konfigurationsdaten automatisch über OpenID Connect Discovery ermittelt werden können:
 - a. Wählen Sie **Automatische Konfigurationsdatenermittlung**.
 - b. Geben Sie im Eingabefeld die Adresse (URL) für die automatische Ermittlung der Konfigurationsdaten an oder wählen Sie über das Pfeilmenü eine Beispieladresse.
 - c. Klicken Sie **Ausführen**.
 - d. Die Konfigurationsdaten werden ermittelt und in einem Dialogfenster angezeigt. Um die Konfigurationsdaten zu übernehmen, klicken Sie **OK**.
 - Sollen die Konfigurationsdaten nicht automatisch ermittelt werden, wählen Sie **Manuelle Dateneingabe**.
Sie müssen die Konfigurationsdaten auf den nächsten Seiten des Assistenten manuell eingeben.
7. Klicken Sie **Weiter**.
8. Auf der Seite **Konfigurationsdaten** erfassen Sie die allgemeinen Informationen zum Identitätsanbieter.

HINWEIS: Haben Sie die automatische Konfigurationsdatenermittlung gewählt, dann sind einige der Informationen bereits ausgefüllt.

Tabelle 36: Allgemeine Konfigurationsdaten des Identitätsanbieters

Eigenschaft	Beschreibung
Anmeldeendpunkt	Uniform Resource Locator (URL) der erweiterten Anmeldeseite des Sicherheitstokendienstes. Beispiel: http://localhost/rsts/login

Eigenschaft	Beschreibung
Abmeldeendpunkt	URL des Abmeldeendpunktes. Beispiel: http://localhost/rsts/login?wa=wsignout1.0
Tokenendpunkt	URL des Tokenendpunktes des Autorisierungsservers für die Rückgabe des Zugriffstokens an den Client für die Anmeldung. Beispiel: https://localhost/rsts/oauth2/token
UserInfo-Endpunkt	URL des OpenID Connect UserInfo-Endpunktes.
Selbstsignierte Zertifikate zulässig	Angabe, ob die Nutzung von selbstsignierten Zertifikaten bei der Verbindung zum Tokenendpunkt und User Info-Endpunkt erlaubt ist.
Aussteller	Uniform Resource Identifier (URI) des Ausstellers des Zertifikates zur Prüfung des Sicherheitstokens. Beispiel: urn:RSTS/identity
Scope	Protokoll für die Authentifizierung. Ist der Wert openid , wird OpenID Connect zur Authentifizierung verwendet, ansonsten wird OAuth 2.0 verwendet.
Shared Secret	Shared-Secret-Wert, der für die Authentifizierung am Tokenendpunkt genutzt wird. Wenn alle Anwendungen des Identitätsanbieters dasselbe Shared Secret nutzen, tragen Sie hier den Wert ein. Nutzen die Anwendungen unterschiedliche Shared Secrets, dann erfassen Sie die Shared-Secret-Werte beim Erstellen der Anwendungen.

9. Klicken Sie **Weiter**.
10. Auf der Seite **Zertifikate konfigurieren** erfassen Sie die Informationen zum Zertifikat des Identitätsanbieters. Wenn alle Anwendungen dasselbe Zertifikat nutzen, tragen Sie hier die Informationen ein. Nutzen die Anwendungen unterschiedliche Zertifikateinstellungen, dann erfassen Sie die Informationen beim Erstellen der Anwendung.

HINWEIS: Haben Sie die automatische Konfigurationsdatenermittlung gewählt, dann sind einige der Informationen bereits ausgefüllt.

Tabelle 37: Informationen zum Zertifikat des Identitätsanbieters

Eigenschaft	Beschreibung
Zertifikatsendpunkt	Uniform Resource Locator (URL) des Zertifikatsendpunkts auf dem Autorisierungsserver. Beispiel: https://localhost/RSTS/SigningCertificate

Eigenschaft	Beschreibung
Subjekt des Zertifikates	Subjekt des Zertifikats, das zur Überprüfung verwendet wird. Subjekt oder Fingerabdruck müssen gesetzt sein.
Fingerabdruck	Fingerabdruck des zu verwendenden Zertifikates zur Prüfung des Sicherheitstokens.
JSON-Web-Key-Endpunkt	URL des JSON-Web-Key-Endpunktes, der die Signierungsschlüssel liefert.
Zertifikat	Inhalt des Zertifikats Zeichenkette. Es wird nur benutzt, wenn kein Zertifikatsendpunkt konfiguriert ist.

11. Klicken Sie **Weiter**.
12. Auf der Seite **Suchregel für Benutzerinformationen** legen Sie fest, wie die Anmeldeinformationen zwischen Identitätsanbieter und One Identity Manager-Datenbank ermittelt werden.

Tabelle 38: Ermitteln der Anmeldeinformationen

Eigenschaft	Beschreibung
Wert für die Suche	<p>Kompletter Name des Claim-Typs aus dem beim Identitätsanbieter die Anmeldeinformationen ermittelt werden.</p> <p>Beispiel: Name einer Entität</p> <p>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</p> <p>Haben Sie die Konfigurationsdaten automatisch ermittelt, wählen Sie einen Wert aus der Liste.</p>
Spalte für die Suche	<p>Tabelle und Spalte in der One Identity Manager-Datenbank in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens UID_Person enthalten, der auf die Tabelle Person zeigt.</p> <p>Beispiel: ADSAccount.ObjectGUID</p>
Wert für Benutzernamen	<p>Kompletter Name des Claim-Typs aus dem beim Identitätsanbieter der Benutzername ermittelt wird. Der Benutzername wird beispielsweise dazu verwendet Datenänderungen im One Identity Manager zu kennzeichnen (Spalten XUserInserted und XUserUpdated).</p> <p>Beispiel: User Principal Name (UPN)</p> <p>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn</p> <p>Haben Sie die Konfigurationsdaten automatisch ermittelt, wählen Sie einen Wert aus der Liste.</p>


13. Klicken Sie **Weiter**.
14. Auf der Seite **OAuth 2.0/OpenID Connect Anwendungen erstellen** erfassen Sie die Informationen zur Anwendung beim Identitätsanbieter.
 - a. Klicken Sie neben dem Eingabefeld Anwendungen auf die Schaltfläche .
 - b. Auf dem Tabreiter **Allgemein** erfassen Sie allgemeinen Informationen zur Anwendung.

Tabelle 39: Allgemeine Informationen zur Anwendung

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Anwendung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Client ID	ID der Anwendung beim Identitätsanbieter. Für native Anwendungen aktivieren Sie die Option Standard . Beispiel: urn:OneIdentityManager/Web
Shared Secret	Anwendungsspezifischer Shared-Secret-Wert, der für die Authentifizierung am Tokenendpunkt genutzt wird.
Abzufragende Ressource	URN der abzufragenden Ressource, zum Beispiel für ADFS. Wird nur benötigt, wenn der Identitätsanbieter diesen Wert erfordert.
Weiterleitungs-URL	Weiterleitungsadresse zur Weiterleitung für Anwendungen. Beispiel: urn:InstalledApplication
Standard	Angabe, ob es sich um eine Standardanwendung für native Anwendungen handelt.

- c. Auf dem Tabreiter **Zertifikat** erfassen Sie die Informationen zum Zertifikat der Anwendung.

Tabelle 40: Informationen zum Zertifikat der Anwendung

Eigenschaft	Beschreibung
Zertifikatsendpunkt	Uniform Resource Locator (URL) des Zertifikatsendpunkts auf dem Autorisierungsserver. Beispiel: https://localhost/RSTS/SigningCertificate
Fingerabdruck	Fingerabdruck des zu verwendenden Zertifikates zur Prüfung des Sicherheitstokens.
Subjekt des Zertifikates	Subjekt des Zertifikats, das zur Überprüfung verwendet wird. Subjekt oder Fingerabdruck müssen gesetzt sein.

Eigenschaft	Beschreibung
Zertifikat	Inhalt des Zertifikats. Es wird nur benutzt, wenn kein Zertifikatsendpunkt konfiguriert ist.

- d. Auf dem Tabreiter **Authentifizierung** erfassen Sie folgende Informationen:

Tabelle 41: Informationen zur Authentifizierungsmethode

Eigenschaft	Beschreibung
Authentifizierungsmethode	Authentifizierungsmethode am Tokenendpunkt. Zulässige Werte sind: <ul style="list-style-type: none"> • client_secret_basic (Standardwert): HTTP Basisauthentifizierungsmethode. Das Shared Secret wird im HTTP Header übergeben. • client_secret_post: Das Shared Secret wird im Wert client_secret des POST-Bodys übergeben. • none: Keine Authentifizierung am Tokenendpunkt. • client_secret_jwt: Das Shared Secret wird als JSON Web Token (JWT) übergeben. • private_key_jwt: Das Shared Secret wird als JWT übergeben. Zusätzlich erfolgt eine Verschlüsselung mit dem privatem Schlüssel.
Tokenendpunkt Zertifikat	Hexadezimaler Fingerabdruck des Zertifikates zur Prüfung des Tokens.

- Um den Identitätsanbieter und die Anwendung in der One Identity Manager-Datenbank zu erstellen, klicken Sie **Weiter**.
- Um den Assistenten zu beenden, klicken Sie **Fertig**.

OAuth 2.0/OpenID Connect Konfiguration an Webanwendungen zuweisen

Um die Authentifizierungsmodule **OAuth2.0/OpenID Connect** und **OAuth2.0/OpenID Connect (rollenbasiert)** in den Webanwendungen des One Identity Manager zu nutzen,

weisen Sie OAuth2.0/OpenID Connect Anwendung an die Webanwendung zu.

Um eine OAuth2.0/OpenID Connect Anwendung an eine Webanwendung zuzuweisen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Webserver Einstellungen**.
2. Wählen Sie im Listeneditor die Webanwendung.
3. Weisen Sie in der Bearbeitungsansicht **Eigenschaften** in der Auswahlliste **OAuth2.0/OpenID Connect Anwendung** die Anwendung zu.
4. Speichern Sie die Änderungen.

TIPP: Für einige Webanwendungen, wie beispielsweise das Web Portal, können Sie die OAuth2.0/OpenID Connect Konfiguration in der Konfigurationsdatei (web.config) anpassen. Ausführliche Informationen Konfiguration des Web Portal finden Sie im *One Identity Manager Installationshandbuch*.

Konfiguration des Identitätsanbieters und der OAuth 2.0/OpenID Connect Anwendungen anzeigen

Um die Konfiguration eines Identitätsanbieters anzuzeigen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | OAuth 2.0/OpenID Connect Konfiguration**.
2. Wählen Sie im Listeneditor den Identitätsanbieter. Die Konfigurationsdaten werden in der Bearbeitungsansicht auf folgenden Tabreitern angezeigt.
 - **Allgemein:** Zeigt die allgemeinen Konfigurationsdaten des Identitätsanbieters.
 - **Zertifikat:** Zeigt die Informationen zum Zertifikat des Identitätsanbieters.
 - **Anwendungen:** Zeigt die Konfiguration der OAuth 2.0/OpenID Connect Anwendungen.
 - **Aktivierende Spalten:** Zeigt die Tabelle und die Spalten, die ein Benutzerkonto als aktiviert kennzeichnen.
 - **Deaktivierende Spalten:** Zeigt die Tabelle und die Spalten, die ein Benutzerkonto als deaktiviert kennzeichnen.

Um die Konfiguration einer OAuth 2.0/OpenID Connect Anwendung anzuzeigen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | OAuth 2.0/OpenID Connect Konfiguration**.
2. Wählen Sie im Listeneditor den Identitätsanbieter.

3. Wählen Sie in der Bearbeitungsansicht den Tabreiter **Anwendungen**.
4. Um die Konfiguration einer Anwendung anzuzeigen, wählen Sie im Bereich **Anwendung** die OAuth 2.0/OpenID Connect Anwendung.

HINWEIS:

Über die Schaltfläche **Hinzufügen** können Sie eine neue OAuth 2.0/OpenID Connect Anwendung zur Konfiguration des Identitätsbieters hinzufügen.

Über die Schaltfläche **Entfernen** können Sie eine nicht mehr benötigte OAuth 2.0/OpenID Connect Anwendung aus der Konfiguration des Identitätsbieters entfernen.

Verwandte Themen

- [OAuth 2.0/OpenID Connect Konfiguration erstellen](#) auf Seite 117
- [Aktivierende und deaktivierende Spalten für die Anmeldung festlegen](#) auf Seite 123

Aktivierende und deaktivierende Spalten für die Anmeldung festlegen

Bei der Ermittlung des Benutzerkontos für die OAuth 2.0/OpenID Connect Authentifizierung wird geprüft, ob das Benutzerkonto aktiviert oder deaktiviert ist. Legen Sie fest, welche Spalten ein Benutzerkonto als aktiviert oder als deaktiviert kennzeichnen.

Beachten Sie:

- Es werden nur die Spalten der Tabelle angeboten, welche Sie in der OAuth 2.0/OpenID Connect Konfiguration des Identitätsanbieters in der **Spalte für die Suche** ausgewählt haben.
- Eine Spalte kann entweder als aktivierende Spalte oder als deaktivierende Spalte genutzt werden.
- Sie können nur aktivierende Spalten oder nur deaktivierende Spalten oder eine Kombination aus aktivierenden und deaktivierenden Spalten festlegen.

Beispiel

Die Spalte für die Suche bezieht sich auf die Tabelle ADSAccount.

Fall a) Die Anmeldung soll nur für aktive Active Directory Benutzerkonten erlaubt sein.

- Wählen Sie als deaktivierende Spalte `ADSAccount.AccountDisabled`.

Wenn am Benutzerkonto die Spalte `ADSAccount.AccountDisabled` gesetzt ist, dann ist die Anmeldung nicht erlaubt.

Fall b) Die Anmeldung soll nur erlaubt sein, wenn es sich um ein privilegiertes Active Directory Benutzerkonto handelt.

- Wählen Sie als aktivierende Spalte `ADSAccount.IsPrivilegedAccount`.

Wenn am Benutzerkonto die Spalte `ADSAccount.IsPrivilegedAccount` gesetzt ist, dann ist die Anmeldung erlaubt.

Fall c) Die Anmeldung soll nur für aktive, privilegierte Active Directory Benutzerkonten erlaubt sein.

- Wählen Sie als aktivierende Spalte `ADSAccount.IsPrivilegedAccount` und als deaktivierende Spalte `ADSAccount.AccountDisabled`.

Wenn am Benutzerkonto die Spalte `ADSAccount.IsPrivilegedAccount` gesetzt ist und die Spalte `ADSAccount.AccountDisabled` nicht gesetzt ist, dann ist die Anmeldung erlaubt.

Um festzulegen, welche Spalten ein Benutzerkonto für die Anmeldung aktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | OAuth 2.0/OpenID Connect Konfiguration**.
2. Wählen Sie im Listeneditor die Konfiguration.
3. Wählen Sie im Bearbeitungsbereich den Tabreiter **Aktivierende Spalten**.
4. Weisen Sie im Bereich **Zuordnung hinzufügen** die Spalten zu, die das Benutzerkonto für die Anmeldung aktivieren.
5. Speichern Sie die Änderungen.

Um festzulegen, welche Spalten ein Benutzerkonto für die Anmeldung deaktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | OAuth 2.0/OpenID Connect Konfiguration**.
2. Wählen Sie im Listeneditor die Konfiguration.
3. Wählen Sie im Bearbeitungsbereich den Tabreiter **Deaktivierende Spalten**.
4. Weisen Sie im Bereich **Zuordnung hinzufügen** die Spalten zu, die das Benutzerkonto für die Anmeldung deaktivieren.
5. Speichern Sie die Änderungen.

Informationen für OAuth 2.0/OpenID Connect Authentifizierung aufzeichnen

Zur Unterstützung bei der Fehlersuche zur OAuth 2.0/OpenID Connect Authentifizierung können persönliche Anmeldeinformationen, wie beispielsweise Informationen zum Token oder zum Aussteller, aufgezeichnet werden. Die Aufzeichnung erfolgt in der Objektprotokolldatei der jeweiligen One Identity Manager-Komponente <appName>_object.log.

Um Informationen zur Authentifizierung im Protokoll auszuzeichnen

- Aktivieren Sie im Designer den Konfigurationsparameter **QBM | DebugMode | OAuth2 | LogPersonalInfoOnException**.

Multifaktor-Authentifizierung im One Identity Manager

Tabelle 42: Konfigurationsparameter für die Multifaktor-Authentifizierung

Konfigurationsparameter	Bedeutung
QER Person Defender	Der Konfigurationsparameter legt fest, ob die klassische Starling Two-Factor Authentication Integration unterstützt wird.
QER Person Defender ApiEndpoint	Der Konfigurationsparameter enthält die URL des Starling 2FA API Endpunktes, über den neue Benutzer registriert werden.
QER Person Defender ApiKey	Der Konfigurationsparameter enthält den Abonnementschlüssel Ihres Unternehmens zum Zugriff auf die Starling Two-Factor Authentication Schnittstelle.
QER Person Starling	<p>Der Konfigurationsparameter legt fest, ob One Identity Starling Cloud unterstützt wird.</p> <p>Starten Sie Ihr Abonnement in Ihrem One Identity On-Prem-Produkt und verbinden Sie Ihre On-Prem-Lösungen mit unserer One Identity Starling Cloud-Plattform. Ermöglichen Sie Ihrem Unternehmen den sofortigen Zugriff auf eine Reihe von in der Cloud bereitgestellten Microservices, die die Funktionen Ihrer On-Prem-Lösungen von One Identity erweitern. Wir werden unserer Starling Cloud-Plattform ständig neue Produkte und Funktionen zur Verfügung stellen. Eine kostenlose Testversion unserer One Identity Starling-Angebote sowie die neuesten Produktfeatures erhalten Sie unter cloud.oneidentity.com.</p>
QER Person Starling ApiEndpoint	Der Konfigurationsparameter enthält den Token Endpoint für die Anmeldung an der One Identity Starling software-as-a-service-Plattform. Der Wert wird durch den Starling Konfigurationsassistenten ermittelt.
QER Person Starling	Der Konfigurationsparameter enthält den Credential String

Konfigurationsparameter Bedeutung

ApiKey	für die Anmeldung an der One Identity Starling software-as-a-service-Plattform. Der Wert wird durch den Starling Konfigurationsassistenten ermittelt.
--------	-------------------------------------------------------------------------------------------------------------------------------------------------------

Für bestimmte sicherheitskritische Aktionen im One Identity Manager kann die Multifaktor-Authentifizierung eingerichtet werden. Diese kann beispielsweise für Attestierungen oder für die Entscheidung von Bestellungen im Web Portal genutzt werden.

Für die Multifaktor-Authentifizierung nutzt der One Identity Manager One Identity Starling Two-Factor Authentication. Dieser Service wird standardmäßig über eine One Identity Starling Cloud-Plattform zur Verfügung gestellt. Sollte Ihr Unternehmen keine Starling Cloud nutzen, wählen Sie die klassische Starling Two-Factor Authentication Integration. Über Konfigurationsparameter geben Sie an, welche der beiden Lösungen in Ihrem Unternehmen angewendet wird.

Um die Multifaktor-Authentifizierung nutzen zu können

1. Registrieren Sie Ihr Unternehmen bei Starling Two-Factor Authentication.
Ausführliche Informationen entnehmen Sie der Starling Two-Factor Authentication Dokumentation.
2. Legen Sie fest, welche Authentifizierungslösung genutzt wird.

- Um Starling Cloud zu nutzen
 - a. Starten Sie das Launchpad.
 - b. Wählen Sie **Verbindung zu Starling Cloud** und klicken Sie **Starten**.
Der Starling Cloud Konfigurationsassistent wird gestartet.
 - c. Folgen Sie den Anweisungen des Starling Cloud Konfigurationsassistenten.

Die Konfigurationsparameter unter **QER | Person | Starling** sind aktiviert und die Authentifizierungsinformationen sind eingetragen.

- Um die klassische Starling Two-Factor Authentication Integration zu nutzen
 - a. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | Defender**.
 - Aktivieren Sie den Konfigurationsparameter **QER | Person | Defender | ApiKey** und erfassen Sie als Wert den Abonnementschlüssel Ihres Unternehmens zum Zugriff auf die Starling Two-Factor Authentication Schnittstelle.

Die Standard-URL des Starling 2FA API Endpunktes ist bereits im Konfigurationsparameter **QER | Person | Defender | ApiEndpoint** eingetragen.

3. Aktivieren Sie für die Tabelle PersonHasQERResource die Zuweisung per Ereignis. Weitere Informationen finden Sie unter [Tabelleneigenschaften bearbeiten](#) auf Seite [128](#).

- (Optional) Legen Sie fest, ob der Sicherheitscode über die Starling 2FA App angefordert werden muss. Weitere Informationen finden Sie unter [Sicherheitscode anfordern](#) auf Seite 129.
- (Optional) Legen Sie fest, ob Bestellungen über die Starling 2FA App entschieden werden dürfen. Weitere Informationen finden Sie unter [Entscheidungen über die Starling 2FA App zulassen](#) auf Seite 131.
- Aktivieren Sie im Manager die Leistungsposition **Neues Starling 2FA Token**. Weitere Informationen finden Sie unter [Bestellung des Starling 2FA Tokens vorbereiten](#) auf Seite 129.

Wenn sich die Telefonnummer des Benutzers geändert hat, bestellen Sie den aktuellen Starling 2FA Token ab und bestellen Sie ihn erneut. Wenn der Starling 2FA Token nicht mehr benötigt wird, bestellen Sie ihn ebenfalls ab.

Ausführliche Informationen finden Sie in den folgenden Handbüchern:

Thema	Handbuch
Vorbereitung des IT Shops für die Multifaktor-Authentifizierung	One Identity Manager Administrationshandbuch für IT Shop
Einrichten der Multifaktor-Authentifizierung für Attestierung	One Identity Manager Administrationshandbuch für Attestierungen
Einrichten der Starling Two-Factor Authentication im Webprojekt	One Identity Manager Konfigurationshandbuch für Webanwendungen
Bestellung des Starling 2FA Tokens	
Bestellung von Produkten, die eine Multifaktor-Authentifizierung benötigen	One Identity Manager Anwenderhandbuch für das Web Portal
Entscheiden von Bestellungen mit Multifaktor-Authentifizierung	
Attestierung mit Multifaktor-Authentifizierung	

Tabelleneigenschaften bearbeiten

HINWEIS: Wenn die Option **Zuweisung per Ereignis** aktiviert ist, wird der Prozess `HandleObjectComponent` in die Jobqueue eingestellt, sobald eine Zuweisung einer Ressource an eine Person hinzugefügt oder entfernt wird.

Um die Zuweisung per Ereignis für eine Tabelle zu aktivieren

- Wählen Sie im Designer die Kategorie **One Identity Manager Schema**.
- Wählen Sie die Tabelle `PersonHasQERResource` und starten Sie den Schemaeditor über die Aufgabe **Tabellendefinition anzeigen**.

3. Wählen Sie in der Ansicht **Tabelleneigenschaften** den Tabreiter **Tabelle** und aktivieren Sie die Option **Zuweisung per Ereignis**.
4. Speichern Sie die Änderungen.

Ausführliche Informationen zur Bearbeitung von Tabellendefinitionen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Bestellung des Starling 2FA Tokens vorbereiten

Damit ein One Identity Manager Benutzer die Multifaktor-Authentifizierung nutzen kann, muss er bei Starling Two-Factor Authentication registriert sein. Um sich zu registrieren, bestellt der Benutzer im Web Portal das Starling 2FA Token. Sobald die Bestellung genehmigt ist, erhält er einen Link zur Starling Two-Factor Authentication App und eine Starling 2FA Benutzerkennung. Mit der App können die Sicherheitscodes generiert werden, die für die Authentifizierung benötigt werden. Die Starling 2FA Benutzerkennung wird in den Personenstammdaten des Benutzers gespeichert.

HINWEIS: In den Personenstammdaten des Benutzers müssen Standard-E-Mail-Adresse, Mobiltelefon und Land hinterlegt sein. Diese Angaben werden für die Registrierung benötigt.

Um die Bestellung des Starling 2FA Tokens zu ermöglichen

1. Wählen Sie die Kategorie **IT Shop | Servicekatalog | Vordefiniert**.
2. Wählen Sie in der Ergebnisliste **Neues Starling 2FA Token**.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Deaktivieren Sie **Nicht bestellbar**.
5. Speichern Sie die Änderungen.

Die Bestellung des Starling 2FA Tokens muss durch den Manager des Empfängers der Bestellung genehmigt werden.

Sicherheitscode anfordern

Tabelle 43: Konfigurationsparameter für die Anforderung des Starling 2FA Sicherheitscodes

Konfigurationsparameter	Bedeutung
QER Person Defender DisableForceParameter	Die Konfigurationsparameter legen fest, ob Starling 2FA gezwungen werden soll, den Sicherheitscode per SMS oder

Konfigurationsparameter Bedeutung

QER Person Starling DisableForceParameter	Telefonanruf zu senden, wenn für die Multifaktor-Authentifizierung eine dieser Optionen ausgewählt ist. Wenn die Konfigurationsparameter aktiviert sind, kann Starling 2FA diese Anforderung zurückweisen; der Benutzer muss dann den Sicherheitscode über die Starling 2FA App anfordern.
-------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Wenn für eine Attestierung, Bestellung oder die Entscheidung einer Bestellung der Sicherheitscode angefordert wird, entscheidet der Benutzer, auf welchem Weg der Sicherheitscode zugestellt wird. Folgende Möglichkeiten können genutzt werden:

- Über die Starling 2FA App
- Per SMS
- Per Telefonanruf

Standardmäßig wird Starling 2FA gezwungen den Sicherheitscode per SMS oder Telefonanruf zu senden, wenn der Benutzer eine dieser Optionen ausgewählt hat. Aus Sicherheitsgründen sollte der Benutzer jedoch die Starling 2FA App nutzen, um den Sicherheitscode zu generieren. Wenn die App auf dem Mobiltelefon des Benutzers installiert ist, kann Starling 2FA die Anforderung von SMS oder Telefonanruf zurückweisen. Der Benutzer muss dann den Sicherheitscode über die App generieren.

Um dieses Verhalten zu nutzen

- Wenn Sie Starling Cloud nutzen, aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | Starling | DisableForceParameter**.
- ODER -
- Wenn Sie die klassische Starling Two-Factor Authentication Integration nutzen, aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | Defender | DisableForceParameter**.

Starling 2FA kann die Übermittlung des Sicherheitscodes per SMS oder Telefonanruf zurückweisen, wenn auf dem Mobiltelefon die Starling 2FA App installiert ist. Der Sicherheitscode muss dann über die App generiert werden.

Wenn der Konfigurationsparameter deaktiviert ist (Standard), wird Starling 2FA gezwungen, den Sicherheitscode per SMS oder Telefonanruf zu senden.

Entscheidungen über die Starling 2FA App zulassen

Tabelle 44: Konfigurationsparameter für die Entscheidung per Starling 2FA App

Konfigurationsparameter	Bedeutung
QER Person Starling UseApprovalAnywhere	Der Konfigurationsparameter definiert, ob Bestellungen über die Starling 2FA App entschieden werden können.
QER Person Starling UseApprovalAnywhere SecondsToExpire	Der Konfigurationsparameter gibt die Wartezeit in Sekunden an, bevor eine Entscheidung per Starling 2FA App abläuft.

Um Entscheidern, die zeitweilig keinen Zugang zu den One Identity Manager Werkzeugen haben, die Möglichkeit zu geben, Bestellungen zu entscheiden, können Sie die Entscheidung per Starling 2FA App zulassen. Dabei werden die Entscheider durch die Starling 2FA App aufgefordert eine Bestellung zu genehmigen oder abzulehnen. Diese Möglichkeit steht zur Verfügung, wenn Sie Starling Cloud für die Multifaktor-Authentifizierung nutzen und die Entscheider bei Starling Two-Factor Authentication registriert sind.

Um die Starling 2FA App für Entscheidungen zu nutzen

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | Starling | UseApprovalAnywhere**.

Die Entscheidung muss in der App standardmäßig innerhalb von 5 Minuten ausgeführt werden. Ist diese Zeit überschritten, muss das Web Portal genutzt werden, um die Bestellung zu entscheiden.

Um diese Wartezeit zu ändern, passen Sie den Wert des Konfigurationsparameters **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** an. Erfassen Sie die Wartezeit in Sekunden.

Abgestufte Berechtigungen für SQL Server und Datenbank

Für den Einsatz einer One Identity Manager-Datenbank oder einer One Identity Manager History Database auf einem SQL Server oder in einer verwalteten Instanz in Azure SQL-Datenbank werden SQL Server Anmeldungen und Datenbankbenutzer für den administrative Benutzer, die Konfigurationsbenutzer und die Endbenutzer bereitgestellt. Die Berechtigungen auf Serverebene und Datenbankebene sind auf die Aufgaben der Benutzer abgestimmt.

In der Regel müssen die Benutzer und Berechtigungen nicht bearbeitet werden. Für den Einsatz einer One Identity Manager History Database kann es erforderlich sein, einen zusätzlichen Datenbankbenutzer einzurichten.

Ausführliche Informationen zu den Benutzern und ihren Berechtigungen finden Sie im *One Identity Manager Installationshandbuch* und im *One Identity Manager Administrationshandbuch für die Datenarchivierung*.

Verwandte Themen

- [Minimale Berechtigungsebenen der One Identity Manager-Werkzeuge](#) auf Seite 132
- [Anmeldungen für den Datenbankserver anzeigen](#) auf Seite 135
- [Berechtigungsebene des Benutzers anzeigen](#) auf Seite 135
- [Berechtigungen der Serverrollen und Datenbankrollen anzeigen](#) auf Seite 136

Minimale Berechtigungsebenen der One Identity Manager-Werkzeuge

HINWEIS:

- Verbindungen, die nicht die erwartete Berechtigungsebene für SQL Server-Anmeldungen verwenden, werden nicht im Verbindungsdialog angezeigt.

- Wenn Sie im Verbindungsdialog eine vorhandene Datenbankverbindung wählen, wird die Berechtigungsebene der verwendeten Anmeldung im Toolltip angezeigt.

Die folgenden minimalen Berechtigungsebenen werden für die One Identity Manager-Werkzeuge benötigt.

Tabelle 45: Berechtigungsebenen der One Identity Manager-Werkzeuge

Werkzeug	Minimale Berechtigungsebene
Analyzer	Endbenutzer
Anwendungsserver	Endbenutzer oder Konfigurationsbenutzer (abhängig von der Aufgabe des Anwendungsservers)
AppServer.Installer.CMD.exe	Konfigurationsbenutzer
API Designer	Konfigurationsbenutzer
API Server	Endbenutzer
Configuration Wizard	Administrativer Benutzer
Crypto Configuration	Konfigurationsbenutzer
Data Import	Endbenutzer Konfigurationsbenutzer (Speichern der Importdefinition)
DataImporterCMD.exe	Endbenutzer
Database Compiler	Konfigurationsbenutzer
DBCompilerCMD.exe	Konfigurationsbenutzer
Database Transporter	Konfigurationsbenutzer
DBTransporterCMD.exe	Administrativer Benutzer
DBClone	Administrativer Benutzer
DBComparer	Konfigurationsbenutzer
Designer	Konfigurationsbenutzer
Job Queue Info	Konfigurationsbenutzer
Launchpad	Endbenutzer Einige der Anwendungen, die aus dem Launchpad gestartet werden, benötigen abweichende Berechtigungsebenen.
License Meter	Endbenutzer
Manager	Endbenutzer Einige Funktionen benötigen die Berechtigungsebene

Werkzeug	Minimale Berechtigungsebene
	für Konfigurationsbenutzer, beispielsweise die Konsistenzprüfung oder das Öffnen der Synchronisationsprojekte für Zielsysteme.
HistoryDB Manager	Endbenutzer
Object Browser	Endbenutzer
One Identity Manager Service	Konfigurationsbenutzer für die Prozessabholung über MSSQLJobProvider
Report Editor	Konfigurationsbenutzer
Schema Extension	Konfigurationsbenutzer
SchemaExtensionCmd.exe	Konfigurationsbenutzer
Server Installer	Konfigurationsbenutzer
Software Loader	Konfigurationsbenutzer
SoftwareLoaderCMD.exe	Konfigurationsbenutzer
Synchronization Editor	Konfigurationsbenutzer
System Debugger	Konfigurationsbenutzer
Web Designer	Konfigurationsbenutzer
Web Designer Configuration Editor	Konfigurationsbenutzer
VI.WebDesigner.CompilerCmd.exe	Konfigurationsbenutzer
WebDesigner.InstallerCMD.exe	Konfigurationsbenutzer
Web Portal	Endbenutzer
Kennwörterücksetzungsportal	Endbenutzer
Web Portal für Betriebsunterstützung	Endbenutzer
Quantum.MigratorCmd.exe	Administrativer Benutzer

Verwandte Themen

- [Abgestufte Berechtigungen für SQL Server und Datenbank](#) auf Seite 132

Anmeldungen für den Datenbankserver anzeigen

Um Informationen für eine Anmeldung anzuzeigen


1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Datenbankserverberechtigungen | Datenbankserver-Anmeldungen**.
2. Wählen Sie die Datenbankserver-Anmeldung. Es werden folgende Informationen werden abgebildet:
 - **Anmeldename:** SQL Server Anmeldung des Benutzers.
 - **Datenbankbenutzer:** Name des Datenbankbenutzers.
 - **Berechtigungsebene:** Berechtigungsebene der Anmeldung. Es werden die Berechtigungsebenen **Endbenutzer**, **Konfigurationsbenutzer**, **Administrativer Benutzer**, **Systemadministrator** und **Unbekannt** abgebildet.
3. Um die zugewiesenen Datenbankrollen und Serverrollen anzuzeigen, wählen Sie den Tabreiter **Datenbank- oder Serverrolle**.

Berechtigungsebene des Benutzers anzeigen

HINWEIS:

- Wenn Sie im Anmeldedialog eine vorhandene Datenbankverbindung wählen, wird die Berechtigungsebene der verwendeten Anmeldung im Tooltip angezeigt.
- Einige Frontends erwarten mindestens die Berechtigungen eines Konfigurationsbenutzers. Die Anmeldung als Endbenutzer wird in diesem Fall nicht unterstützt.

Um die Berechtigungsebene für den angemeldeten Benutzer zu ermitteln

- Um die Benutzerinformationen anzuzeigen, doppelklicken Sie in der Statuszeile des Programms auf das Symbol 

Auf dem Tabreiter **Systembenutzer** wird im Eingabefeld **SQL Berechtigungslevel** die Berechtigungsebene der verwendeten Anmeldung angezeigt. Es werden die Berechtigungsebenen **Endbenutzer**, **Konfigurationsbenutzer**, **Administrativer Benutzer**, **Systemadministrator** und **Unbekannt** abgebildet.

Verwandte Themen

- [Anmeldungen für den Datenbankserver anzeigen](#) auf Seite 135

Berechtigungen der Serverrollen und Datenbankrollen anzeigen

Die Berechtigungen der Serverrollen und Datenbankrollen sind vordefiniert und können nicht bearbeitet werden.

HINWEIS: Für kundenspezifische Schemaerweiterungen wird die Datenbankrolle **Rolle für Endbenutzer** berechtigt.

Um die Berechtigungen der Serverrollen und Datenbankrollen anzuzeigen

- Wählen Sie im Designer in der Kategorie **Basisdaten | Sicherheitseinstellungen | Datenbankserverberechtigungen | Datenbankserver-Anmeldungen** die Serverrolle oder die Datenbankrolle.

Im Listeneditor werden die einzelnen Berechtigungen angezeigt.

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 Geschäftssagilität 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

A

Anwendung

- Authentifizierungsmodul zuweisen 103
- Konfigurationsdaten 109
- Rechtegruppe zuweisen 63

Anwendungsrolle 8

- Administratoren 10, 13-14, 16-21, 23-25
- Attestierer 13-14, 18-19, 21
- Attestierer für externe Benutzer 16
- Auditoren 12
- Ausnahmegenehmiger 14
- Basisrollen 10
 - Administratoren 10, 26
 - Betriebsunterstützung 10
 - Interne Berechtigungen 10
 - Jeder (Ändern) 10
 - Jeder (Sehen) 10
 - Personenverantwortliche 10

bearbeiten 27-28

Bearbeitungsrechte erweitern 30

Benutzerspezifisch 25

- Administratoren 25

- Verantwortliche 25

Berechtigten als One Identity Manager Administrator 26

Berichte 34

Berichte zuweisen 33

Cloud-Administratoren 24

Compliance und Security Officer 12

dynamisch 31

Führungsebene 18

Genehmiger 18-19

Genehmiger (IT) 18-19

Identity Management 18

- Führungsebene 18

- Geschäftsrollen 18

- Administratoren 18

- Attestierer 18

- Genehmiger 18

- Genehmiger (IT) 18

Organisationen 19

- Administratoren 19

- Attestierer 19

- Genehmiger 19

- Genehmiger (IT) 19

Personen 20

- Administratoren 20

Identity und Access Governance 12-14, 16-17

Abonnierbare Berichte 17

- Administratoren 17

Attestierung 16

- Administratoren 16

- Zentrale Entscheidergruppe 16

Auditoren 12

Compliance & Security Officer 12

Identity Audit 13

- Administratoren 13

- Attestierer 13

- Pflege SAP Funktionen 13

- Regelverantwortliche 13

- Unternehmensrichtlinien 14
 - Administratoren 14
 - Attestierer 14
 - Ausnahmegenehmiger 14
 - Richtlinienverantwortliche 14
- Inbetriebnahme 26
- Interne Berechtigungen 10
- Personen zuweisen 29, 31
- Personenverantwortliche 10
- Produkteigner 21
- Rechtegruppe 28, 30
- Regelverantwortliche 13
- Request und Fulfillment 21
 - IT Shop 21
 - Administratoren 21
 - Attestierer 21
 - Produkteigner 21
 - Zentrale Entscheidergruppe 21
- Richtlinienverantwortliche 14
- Selbstregistrierte Personen 10
- Überblick 9
- Universal Cloud Interface
 - Administratoren 24
- widersprechende 32
- Zentrale Entscheidergruppe 16, 21
- Zielsysteme
 - Administratoren 23
 - Zielsystemverantwortliche 23
- Zielsystemverantwortliche 23
- Zusatzeigenschaft zuweisen 33
- Authentifizierung
 - überprüfen 114
- Authentifizierungsmodul
 - Active Directory Benutzerkonto 81
 - Active Directory Benutzerkonto
 - (dynamisch) 86
 - Active Directory Benutzerkonto (manuell) 83
 - Active Directory Benutzerkonto (manuelle Eingabe/rollenbasiert) 84
 - Active Directory Benutzerkonto (rollenbasiert) 82
 - aktivieren 102
 - Anwendung zuweisen 103
 - Benutzerkonto 78
 - Benutzerkonto (rollenbasiert) 79
 - Component Authenticator 97
 - Crawler 97
 - HTTP Header 91
 - HTTP Header (rollenbasiert) 92
 - Initiale Daten 105
 - Kennworrücksetzung 98
 - Kennworrücksetzung (rollenbasiert) 99
 - Kontobasierter Systembenutzer 80
 - LDAP Benutzerkonto (dynamisch) 89
 - LDAP Benutzerkonto (rollenbasiert) 87
 - OAuth 2.0/OpenID Connect 93
 - OAuth 2.0/OpenID Connect (rollenbasiert) 94
 - Person 75
 - Person (dynamisch) 77
 - Person (rollenbasiert) 76
 - Single Sign-on generisch (rollenbasiert) 73
 - Synchronisationsauthenticator 96
 - Systembenutzer 73
 - Web Agent Authenticator 96

B

Benutzer

- Authentifizierungsmodul 62
- Berechtigungen 62
- Berechtigungsebene 135
- dynamischer 62
- Leserechte 62
- Programmfunktion 62
- Rechtegruppen 62
- Systembenutzer 62

Berechtigungen

- Benutzer 62
- Datenbank 132
- Datenbankrolle 136
- Objekt 61
- Rechtegruppe 54
- Regeln 40
- Serverrolle 136
- SQL Server 132
- Tabelle 54

D

Datenbankrolle

- Berechtigungen anzeigen 136

Datenbankserver

- Anmeldung 135
- Berechtigungen 132
- Berechtigungsebene 135
- Datenbankbenutzer 135

Dynamische Rolle

- Anwendungsrolle 31

E

Entscheidung

- per App 131

Ereignis

- Objektereignis 69
- Programmfunktion 69

L

Launchpad

- Aktionen
- Programmfunktion 71

M

Methodendefinition

- Programmfunktion 68

Multifaktor-Authentifizierung 126

O

OAuth 2.0/OpenID Connect

- Aktivierende Spalten 123
- Anwendung 117, 122
- Authentifizierung 115
- Authentifizierungsmodul 93-94
- Deaktivierende Spalten 123
- Identitätsanbieter 117, 122
- Konfiguration 115, 117, 122
- openid 117
- Scope 117
- Shared Secret 117
- Webanwendung 121
- Zertifikat 117

- Objekt
 - Berechtigungen 61
 - Objekt ereignis 69
 - Programmfunktion 69
 - One Identity Starling software-as-a-service 126
- P**
- Person
 - Berechtigungen als One Identity Manager Administrator 26
 - Programmfunktion 64, 67, 69
 - Launchpad Aktionen 71
 - Methodendefinition 68
 - Rechtegruppe 67-69
 - Skript 67
- R**
- Rechte
 - bearbeiten 53
 - Berechtigungsfilter 55
 - ermitteln 40
 - kopieren 58
 - Regeln 40
 - Simulation 59
 - Spaltenrechte 57
 - Tabellenrechte 55
 - Rechteeditor 53
 - Rechtegruppe
 - Abhängigkeiten 44-45
 - Anwendung zuweisen 63
 - Berechtigungen 54
 - einrichten 42-43, 47
 - Hierarchie 44
 - kopieren 46
 - Nur für rollenbasierte Anmeldung 43
 - Programmfunktion 67-69
 - QBM_BaseRights 37
 - QER_OperationsSupport 37
 - rollenbasiert 37
 - vi_4_ADMIN_LOOKUP 37
 - VI_4_ALLUSER 37
 - VI_Everyone 37
 - VI_View 37
 - vid 37
 - VID_Features 37
 - vordefiniert 37
- S**
- Serverrolle
 - Berechtigungen anzeigen 136
 - Sicherheitscode
 - anfordern
 - per Anruf 129
 - per App 129
 - per SMS 129
 - Skript
 - Berechtigung 67
 - Programmfunktion 67
 - Starling 2FA 126, 129
 - Starling 2FA Sicherheitscode 129
 - Starling Cloud 126
 - Starling Cloud Sicherheitscode 129
 - Starling Two-Factor Authentication 126
 - Systembenutzer
 - Administrativer Benutzer 50
 - Anmeldungen 50
 - Benutzer 52
 - Dienstkonto 50
 - dynamisch 37, 53

- dynamisch ermitteln 109
- einrichten 48-49
- Kennwort 49-50
- Kennwort läuft nie ab 49-50
- Nur Leserechte 50
- Personen 52
- Rechtegruppen 51
- sa 37
- Support 37
- Synchronization 37
- viadmin 37
- viHelpdesk 37
- vordefiniert 37

T

Tabelle

- Berechtigungen 54

Token 129

Z

Zuweisungsressource

- für eine Anwendungsrolle 34