One Identity Manager 8.1

Handbuch zur Autorisierung und Authentifizierung

Legende

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

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

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

One Identity Manager Handbuch zur Autorisierung und Authentifizierung
Aktualisiert - März 2019
Version - 8.1

Inhalt

Über dieses Handbuch

Über das One Identity Manager Rollen-und Berechtigungsmodell werden die Bearbeitungsrechte für die Benutzer des One Identity Manager gesteuert. Die Berechtigungen für den Zugriff auf die Tabellen und Spalten des One Identity Manager Schema werden über Rechtegruppen definiert. Rechtegruppen können mit Anwendungsrollen verknüpft werden. Die Benutzer werden an Anwendungsrollen zugewiesen und erhalten somit die Berechtigungen, die Sie benötigen. Die gültigen Berechtigungen für einen Benutzer werden bei der Anmeldung am One Identity Manager ermittelt. Für die Anmeldung stellt der One Identity Manager verschiedene Authentifizierungsmodule zur Verfügung.

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

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.

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.

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.

2

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 Recht 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 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 auf Seite 36
- One Identity Manager Authentifizierungsmodule auf Seite 73

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
- Anwendungsrollen für abonnierbare 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

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

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

Tabelle 1: Anwendungsrollen für Basisfunktionen

Anwendungsrolle	Beschreibung
Administratoren	Die Administratoren müssen der Anwendungsrolle **Basisrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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 Kennwortrücksetzungsportal für ausgewählte Systembenutzer Kennwörter setzen.
Jeder (Ändern)	Die Anwendungsrolle **Basisrollen | Jeder (Ändern)** wird automatisch jedem Benutzer zugewiesen. Benutzer mit dieser Anwendungsrolle: • Können bestimmte Personenstammdaten im Web Portal bearbeiten. Soll jedem Benutzer bei der Anmeldung automatisch eine kundendefinierte Rechtegruppe zugewiesen werden, so kann diese Rechtegruppe auf dem Stammdatenformular der Anwendungsrolle eingetragen werden. Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.

Anwendungsrolle	Beschreibung
Jeder (Sehen)	Die Anwendungsrolle **Basisrollen | Jeder (Sehen)** wird automatisch jedem Benutzer zugewiesen. Benutzer mit dieser Anwendungsrolle: • Erhalten Leseberechtigungen auf Objekte im Web Portal. Soll jedem Benutzer bei der Anmeldung automatisch eine kundendefinierte Rechtegruppe zugewiesen werden, so kann diese Rechtegruppe auf dem Stammdatenformular der Anwendungsrolle eingetragen werden. Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.
Personenverantwortliche	Die Anwendungsrolle **Basisrollen | Personenverantwortliche** wird einem Benutzer automatisch zugewiesen, wenn der Benutzer Manager oder Verantwortlicher von Personen, Abteilungen, Standorten, Kostenstellen, Geschäftsrollen oder IT Shops ist. Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Stammdaten der Objekte, für die sie verantwortlich sind, und weisen ihnen Unternehmensressourcen zu. • Können im Web Portal die Stammdaten ihrer Mitarbeiter bearbeiten. • Können ihre Mitarbeiter in den IT Shop aufnehmen. • Manager von Personen und Abteilungen können im Web Portal neue Personen anlegen. • Können im Web Portal die Complianceregelverletzungen ihrer Mitarbeiter sehen. Die Mitglieder dieser Anwendungsrolle werden über eine dynamische Rolle ermittelt.
Initiale Berechtigungen	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.
Betriebsunterstützung	Personen, die das Web Portal für Betriebsunterstützung nutzen, müssen der Anwendungsrolle **Basisrollen** | **Betriebs-**

Anwendungsrolle	Beschreibung
	unterstützung zugewiesen werden. Benutzer mit dieser Anwendungsrolle: • überwachen die Verarbeitung von Prozessen der Jobqueue • überwachen die Verarbeitung der DBQueue • erstellen Zugangscodes, um Mitarbeitern zu ermöglichen, sich am Kennwortrücksetzungsportal anzumelden

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 und 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 Compliance-regeln vorhanden ist.

Für die Verwaltung von Complianceregeln sind folgende Anwendungsrollen verfügbar.

Tabelle 2: Anwendungsrollen für Identity Audit

Anwendungsrolle	Beschreibung
Administratoren	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen die Basisdaten für die Erstellung des Regelwerks. • Erstellen die Complianceregeln 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	Die Regelverantwortlichen müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Regelverantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind inhaltlich verantwortlich für Complianceregeln, beispielsweise Wirtschaftsprüfer oder Revisionsabteilung. • Bearbeiten die Arbeitskopien der Complianceregeln, denen die Anwendungsrolle zugeordnet ist. • Aktivieren und deaktivieren Complianceregeln. • Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen. • Weisen risikomindernde Maßnahmen zu.

Anwendungsrolle	Beschreibung
Ausnahmegenehmiger	Die Ausnahmegenehmiger müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Ausnahmegenehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten im Web Portal die Regelverletzungen. • Können im Web Portal Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer	Die Attestierer müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren im Web Portal die Complianceregeln und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Complianceregeln sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Pflege SAP Funktionen	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Pflege SAP Funktionen** oder eine untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul SAP R/3 Compliance Add-on vorhanden ist.

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	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichlinien | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen die Basisdaten für die Erstellung der Unternehmensrichtlinien. • Erstellen die Richtlinien und weist 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	Die Richtlinienverantwortlichen müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Richtlinienverantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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	Benutzer mit dieser Anwendungsrolle: Die Ausnahmegenehmiger müssen der Anwendungsrolle

Anwendungsrolle	Beschreibung
	Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Richtlinienverletzungen. • Können Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer	Die Attestierer müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren im Web Portal die Unternehmensrichtlinien und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Unternehmensrichtlinien sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Anwendungsrollen für Attestierung

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

Für die Verwaltung der Attestierungsverfahren ist folgende Anwendungsrolle verfügbar.

Tabelle 4: Anwendungsrollen für Attestierung

Anwendungsrolle	Beschreibung
Administratoren	Die Administratoren sind der Anwendungsrolle **Identity & Access Governance | Attestierung | Administratoren** zugewiesen. Benutzer mit dieser Anwendungsrolle: • Definieren Attestierungsverfahren und Attestierungsrichtlinien. • Erstellen die Entscheidungsrichtlinien und Entscheidungsworkflows. • Legen fest, nach welchen Entscheidungsverfahren die Attes-

Anwendungsrolle	Beschreibung
	tierer ermittelt werden. • Richten die Benachrichtigungen für Attestierungsvorgänge ein. • Konfigurieren die Zeitpläne für die Attestierungen. • Erfassen risikomindernde Maßnahmen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Überwachen die Attestierungsvorgänge.
Zentrale Entscheidergruppe	Die zentralen Entscheider müssen der Anwendungsrolle **Identity & Access Governance| Attestierung | Zentrale Entscheidergruppe** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über Attestierungsvorgänge. • Weisen Attestierungsvorgänge anderen Attestierern zu.

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.

Anwendungsrollen 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	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Abonnierbare Berichte | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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 abonnierter Berichten per E-Mail.

Führungsebene

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

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 Anwendungsrolle steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Für die Verwaltung der Geschäftsrollen sind folgende Anwendungsrollen verfügbar.

Tabelle 6: Anwendungsrollen für Geschäftsrollen

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

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

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

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. • 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 Standorte, 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 Standorte, für die sie verantwortlich sind.

Anwendungsrollen für Personen

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

Für die Verwaltung der Personen ist folgende Anwendungsrolle verfügbar.

Tabelle 8: Anwendungsrollen für Personen

Anwendungsrolle	Beschreibung
Administratoren	Personenadministratoren müssen der Anwendungsrolle **Identity Management | Personen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Stammdaten aller Personen. • Ordnen den Manager zu. • Weisen Unternehmensressourcen an die Personen zu. • Überprüfen und autorisieren die Stammdaten von Personen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Bearbeiten Kennwortrichtlinien für Kennwörter von Personen.

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	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen die IT Shop-Struktur mit Shops, Regalen, Kunden, Vorlagen und dem Servicekatalog. • Erstellen die Entscheidungsrichtlinien und Entscheidungsworkflows. • Legen fest, nach welchen Entscheidungsverfahren die Entschei-

Anwendungsrolle	Beschreibung
	der ermittelt werden. • Erstellen die Produkte und Leistungspositionen. • Richten die Benachrichtigungen für Bestellvorgänge ein. • Überwachen die Bestellvorgänge. • Administrieren die Anwendungsrollen für Produkteigner und Attestierer. • 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	Die Produkteigner müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über Bestellungen. • Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind.
Attestierer	Die Attestierer müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Zentrale Entscheidergruppe	Die zentralen Entscheider müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Zentrale Entscheidergruppe** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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 widersprechen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | <Zielsystem>** oder einer untergeordneten Anwendungsrolle zugewiesen sein. HINWEIS: Pro Zielsystem gibt es mindestens eine Standardanwendungsrolle für Zielsys-temverantwortliche. Diese Anwendungsrolle stehen zur Verfügung, wenn das Modul für das Zielsystem vorhanden ist. Benutzer mit dieser Anwendungsrolle:

Benutzer	Aufgaben
	• 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. • Können Personen anlegen, die eine andere Identität haben als **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	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Unified Namespace** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erhalten eine zielsystemübergreifende Sicht auf die Objekte der angeschlossenen Zielsysteme. • Können zielsystemübergreifende Berichte erstellen. Sind die Benutzer gleichzeitig Zielsystemverantwortliche der zugrunde liegenden Zielsysteme, können Sie diese Zielsysteme über den Unified Namespace verwalten.

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	Die Administratoren müssen der Anwendungsrolle **Universal Cloud Interface | Administratoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für das Universal Cloud Interface. • 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	Die Operatoren müssen der Anwendungsrolle **Universal Cloud Interface | Operatoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten offene, manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.
Cloud-Auditoren	Die Auditoren müssen der Anwendungsrolle **Universal Cloud Interface | Auditoren** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sehen manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.

Anwendungsrollen für benutzerspezifische Aufgaben

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

Für benutzerspezifische Funktionen und Aufgaben sind folgende Anwendungsrollen verfügbar.

Tabelle 12: Anwendungsrollen für benutzerspezifische Aufgaben

Anwendungsrolle	Beschreibung
Administratoren	Die Administratoren müssen der Anwendungsrolle **Benutzerspezifisch | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die benutzerspezifischen Anwendungsrollen. • Richten bei Bedarf weitere Anwendungsrollen für Verantwortliche ein.
Verantwortliche	Die Verantwortlichen müssen der Anwendungsrolle **Benutzerspezifisch | Verantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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. 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.

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 **Berechtigen als One Identity Manager Administrator**.

HINWEIS: Sobald Sie die Ansicht im Manager aktualisieren, wird die Aufgabe **Berechtigen 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 73

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.
Rechtegruppe	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. Administratoren können den übrigen Anwendungsrollen

Eigenschaft	Bedeutung
	kundendefinierte Rechtegruppen zuordnen. Weitere Informationen finden Sie unter Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen auf Seite 30. HINWEIS: Die Rechtegruppen der Standardanwendungsrollen für Administratoren können nicht bearbeitet werden.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Zertifizierungsstatus	Zertifizierungsstatus der Anwendungsrolle. Folgende Werte können ausgewählt werden. • **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	HINWEIS: Diese Option ist aus Kompatibilitätsgründen zu älteren Programmversionen vorhanden. Es wird empfohlen, die Option nicht zu aktivieren. Gibt an, ob bei Bestellungen im IT Shop mit den Entscheidungsverfahren RD, RL, RO oder RP auch Personen übergeordneter Anwendungsrollen als Entscheider ermittelt werden dürfen. Ist die Option aktiviert, werden nur die Personen als Entscheider ermittelt, die genau dieser Anwendungsrolle zugewiesen sind. Ausführliche Informationen zu den Entscheidungsverfahren im IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
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

- Dynamischen Rollen für Anwendungsrollen erstellen auf Seite 31

Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen

Für die rollenbasierte Anmeldung benötigten 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 auf Seite 36

Zusätzliche Aufgaben für die Verwaltung von Anwendungsrollen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Dynamischen Rollen für Anwendungsrollen erstellen

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.

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 *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
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

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.

Die gültigen Berechtigungen eines Benutzers sind abhängig vom Authentifizierungsmodul, das für die Anmeldung an den One Identity Manager-Werkzeugen verwendet wird.

- 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.

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.

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 43
- Bearbeitung von Systembenutzern auf Seite 48
- Bearbeitung der Tabellenrechte und Spaltenrechte auf Seite 54
- Steuern von Berechtigungen über Programmfunktionen auf Seite 65
- Berechtigungen für Objekte anzeigen auf Seite 62
- Berechtigungen der angemeldeten Benutzer anzeigen auf Seite 63
- Rollenbasierte Rechtegruppen an Anwendungen zuweisen auf Seite 64

Verwandte Themen

- One Identity Manager Anwendungsrollen auf Seite 8
- One Identity Manager Authentifizierungsmodule auf Seite 73

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 Administrationswerkzeugen 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	Beschreibung
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 Schemaerweiterungen zu.
Rechtegruppe **VI_Everyone**	Die Rechtegruppe **VI_Everyone** sind Formularelemente der Übersichtformulare, die Links zu den korrespondieren 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 Übersichtsformulare für den Benutzer vollständig angezeigt werden.
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.

Rechtegruppe	Beschreibung
	HINWEIS: Weisen Sie der Rechtegruppe die Sichtbarkeitsrechte auf kundenspezifischen Schemaerweiterungen 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**	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.

Systembenutzer	Beschreibung
	WICHTIG: Verwenden Sie den Systembenutzer **viadmin** nicht im produktiven Betrieb. Erstellen Sie einen eigenen Systembenutzer mit entsprechenden Berechtigungen. 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.
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.
Systembenutzer **viITShop**	Der Systembenutzer **viITShop** hat die vorgegebenen Berechtigungen und die Benutzeroberfläche, um mit dem Manager auf den IT Shop zuzugreifen.

Verwandte Themen

- Dynamische Systembenutzer löschen auf Seite 53
- Abhängigkeiten zwischen Rechtegruppen auf Seite 44
- Bearbeitung von Rechtegruppen auf Seite 43

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.
- 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
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 kundenspezifische 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, auf 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 44

- Abhängigkeiten von Rechtegruppen bearbeiten auf Seite 45
- Rechtegruppen kopieren auf Seite 46
- Rechtegruppen erstellen auf Seite 48
- Steuern von Berechtigungen über Programmfunktionen auf Seite 65

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.
Binäre 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 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 48

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)

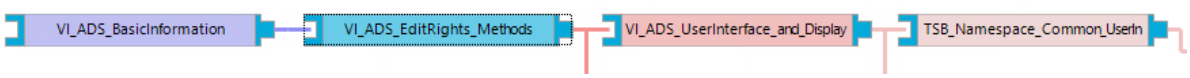

Tabelle 18: Bedeutung der Farben in der hierarchischen Darstellung

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, der sich aus dem Kundenpräfix und dem Namen der ursprünglichen Rechtegruppe zusammensetzt. Sie können diesen Namen anpassen, das Kundenpräfix muss jedoch bestehen bleiben.
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 gewählten Rechtegruppe in die neue Rechtegruppe aufzunehmen. HINWEIS: Beachten Sie hierbei, dass vordefinierte Systembenutzer nicht in die neue Rechtegruppe aufgenommen werden.

7. Um den Kopiervorgang zu starten, klicken Sie **Weiter**.

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

Verwandte Themen

- Rechtegruppen erstellen auf Seite 48
- Eigenschaften von Rechtegruppen auf Seite 44
- Abhängigkeiten von Rechtegruppen bearbeiten auf Seite 45

- Systembenutzer in Rechtegruppen aufnehmen auf Seite 52
- Bearbeitung der Tabellenrechte und Spaltenrechte auf Seite 54

Rechtegruppen erstellen

Um eine Rechtegruppe 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 eine neue Rechtegruppe über das Menü **Rechtegruppen | Neu** ein.
4. Bearbeiten Sie die Stammdaten der Rechtegruppe.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Rechtegruppen kopieren auf Seite 46
- Eigenschaften von Rechtegruppen auf Seite 44
- Abhängigkeiten von Rechtegruppen bearbeiten auf Seite 45
- Systembenutzer in Rechtegruppen aufnehmen auf Seite 52

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 eine 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 50
- Eigenschaften von Systembenutzern auf Seite 50
- Systembenutzer in Rechtegruppen aufnehmen auf Seite 52
- Welche Personen verwenden den Systembenutzer? auf Seite 53
- 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 50
- Eigenschaften von Systembenutzern auf Seite 50

- Systembenutzer in Rechtegruppen aufnehmen auf Seite 52
- Dynamische Systembenutzer löschen auf Seite 53
- Welche Personen verwenden den Systembenutzer? auf Seite 53
- One Identity Manager Authentifizierungsmodule auf Seite 73

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	Angabe, ob das Kennwort abläuft. Aktivieren Sie die Option

Eigenschaft	Beschreibung
ab	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: `Domäne\Benutzer` 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.
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 50

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 Administrationswerkzeugen 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

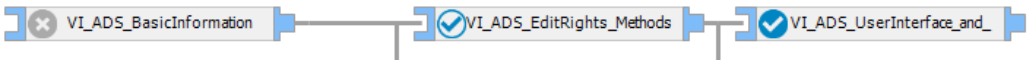

Tabelle 21: Bedeutung der Symbole in der hierarchischen Darstellung

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 Personen 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 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 55
- Berechtigungen für Tabellen anzeigen auf Seite 55
- Tabellenrechte bearbeiten auf Seite 56
- Spaltenrechte bearbeiten auf Seite 58
- Tabellenrechte und Spaltenrechte kopieren auf Seite 59
- Berechtigungen für Systembenutzer simulieren auf Seite 61

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 58
- Tabellenrechte und Spaltenrechte kopieren auf Seite 59

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.

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 56
- Tabellenrechte und Spaltenrechte kopieren auf Seite 59

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

  Es werden alle kopierten Rechte für die Zieltabelle (Zielspalte) eingefügt. Vorhandene Rechte der Zieltabelle (Zielspalte), die nicht für die Quelltabelle (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 56
- Spaltenrechte bearbeiten auf Seite 58

Berechtigungen für Systembenutzer simulieren

Über die Simulation der Rechte im Rechteeditor sehen Sie für einen Systembenutzer, welche Berechtigungen er aufgrund seiner Rechtegruppe 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 implizite Rechte auf die Anzeigewerte der Fremdschlüsselspalten vergeben.

     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 erweitere 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.

Symbol	Bedeutung
	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.
Nur Leserechte	Der verwendete Systembenutzer besitzt nur Leserechte. Datenänderungen sind nicht möglich.

Eigenschaft	Bedeutung
Dynamischer Benutzer	Der angemeldete Benutzer verwendet einen dynamischen Systembenutzer. Dynamische Systembenutzer werden eingesetzt, wenn zur Anmeldung ein rollenbasiertes Authentifizierungsmodul benutzt wird.
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*.

4

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 angemeldete 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 65
- Berechtigungen der angemeldeten Benutzer anzeigen auf Seite 63
- Programmfunktionen an Rechtegruppen zuweisen auf Seite 68
- Berechtigungen zum Ausführen von Skripten auf Seite 68
- Berechtigungen zum Ausführen von Methoden auf Seite 69
- Berechtigungen zum Auslösen von Prozessen auf Seite 71
- Berechtigungen zum Ausführen von Aktionen im Launchpad auf Seite 72

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-rollenbasierte Anmeldung: Nehmen Sie im Designer in der Kategorie **Berechtigungen | Systembenutzer** den Systembenutzer in die Rechtegruppe auf.
- Für rollenbasierte 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 68
- Systembenutzer in Rechtegruppen aufnehmen auf Seite 52
- Personen an Anwendungsrollen zuweisen auf Seite 29

Programmfunktionen eines 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 52

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 zugewiesen hat. 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 sollen.
    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 43

Berechtigungen zum Ausführen von Methoden

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

Programmfunktion zugewiesen hat. Besitzt der Benutzer die Programmfunktion nicht, so wird beim Ausführungsversuch eine Fehlermeldung geworfen. Programmfunktionen werden nicht an einzelne Benutzer, sondern an Rechtegruppen zugewiesen. Alle Benutzer, die dieser Rechtegruppe zugeordnet sind, können die Programmfunktion nutzen.

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 `QBMMethodHasFeature`.
    c. Wählen Sie im Listeneditor die neu erstellte Programmfunktion.
    d. Weisen Sie in der Bearbeitungsansicht **Methoden** die Methodendefinitionenzu.
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 43

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 Objektereignisse (Tabelle `QBMEvent`) mit einer Programmfunktion (Tabelle `QBMFeature`) zu verbinden. Ein Ereignis (Tabelle `JobEventGen`), welches für einen Prozess definiert wird, wird mit einem Objektereignis (Spalte `JobEventGen.UID_QBMEvent`) verknüpft. Wird das Objektereignis mit einer Programmfunktion (Tabelle `QBMEventHasFeature`) versehen, dann können Benutzer, die diese Programmfunktion besitzen, das zugeordnete Objektereignis 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 Objektereignissen, 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 **Objektereignisse** die Objektereignisse 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 43

Berechtigungen zum Ausführen von Aktionen im Launchpad

One Identity Manager liefert eine Reihen 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.

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 Programmfunktion 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.

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	• 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	• 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	Der One Identity Manager sucht laut Konfiguration das Benutzerkonto und 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. 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.

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.
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`

Konfigurationsparameter	Bedeutung
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	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.

Datenänderungen werden der angemeldeten Person zugeordnet.

Person (rollenbasiert)

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

Anmeldeinformationen	Zentrales Benutzerkonto und Kennwort der Person.
Voraussetzungen	• 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	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.

Person (dynamisch)

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

Anmeldeinformationen	Zentrales Benutzerkonto und Kennwort der Person.
Voraussetzungen	• 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 107

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 Frontend möglich	ja
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	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.

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.

Kontobasierter Systembenutzer

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. • 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 Portal möglich	nein
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	• 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	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.

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.

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	• 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 | AuthenticationDomains** eingetragen. • Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abtei-

	lungszugehörigkeit, 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	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. 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.

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	• 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	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. 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.

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	• 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	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. 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.

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 107

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	• 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 des Containers das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Erfolgt die Anmeldung über den definierten Namen, wird dieser direkt 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**.
TargetSystem | LDAP | Authentication | RootDN	Der Konfigurationsparameter enthält den Distinguished Name der Root-Domäne. Syntax: `dc=MyDomain`
TargetSystem | LDAP | Authentication | Server	Der Konfigurationsparameter enthält den Namen des LDAP Servers.

LDAP Benutzerkonto (dynamisch)

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	• 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 des Containers das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Erfolgt die Anmeldung über den definierten Namen, wird dieser direkt 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 | Authentication | RootDN	Der Konfigurationsparameter enthält den Distinguished Name der Root-Domäne. Syntax: `dc=MyDomain`
TargetSystem | LDAP | Authentication | Server	Der Konfigurationsparameter enthält den Namen des LDAP Servers.

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 107

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	• 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: `username = <Benutzername des authentifizierten Benutzers>`) 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	• 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: `username = <Benutzername des authentifizierten Benutzers>`) 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	• 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	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 Bearbeitungsrechte werden über den Systembenutzer geladen, der der ermittelten Person direkt zugeordnet ist. Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet. Dafür muss der Claim-Typ bekannt sein, dessen Wert zur Kennzeichnung der Datenänderungen verwendet wird.

Verwandte Themen

- OAuth 2.0/OpenID Connect Konfiguration auf Seite 113
- Ablauf der OAuth 2.0/OpenID Connect Authentifizierung auf Seite 113

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	• 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	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. Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet. Dafür muss der Claim-Typ bekannt sein,

dessen Wert zur Kennzeichnung der Datenänderungen verwendet wird.

Verwandte Themen

- OAuth 2.0/OpenID Connect Konfiguration auf Seite 113
- Ablauf der OAuth 2.0/OpenID Connect Authentifizierung auf Seite 113

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.

Kennwortrücksetzung

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

Das Authentifizierungsmodul wird zur Anmeldung am Kennwortrücksetzungsportal 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.
Voraussetzungen	• Die Person ist in der One Identity Manager-Datenbank vorhanden. • In den Personenstammdaten ist das zentrale Benutzerkonto 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 Kennwortrücksetzungsportal muss eingetragen sein. Das Anwendungstoken setzen Sie bei der

Installation des Kennwortrücksetzungsportals. 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 Kennwortrücksetzungsportals finden Sie im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Kennwortrücksetzung (rollenbasiert)

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

Das Authentifizierungsmodul wird zur Anmeldung am Kennwortrücksetzungsportal 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.
Voraussetzungen	• Die Person ist in der One Identity Manager-Datenbank vorhanden. • In den Personenstammdaten ist das zentrale Benutzerkonto 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	Das Anwendungstoken für das Kennwortrücksetzungsportal muss eingetragen sein. Das Anwendungstoken setzen Sie bei der Installation des Kennwortrücksetzungsportals. 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 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.

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 Programmfunktion besitzen, die Anwendung zu benutzen.

Detaillierte Informationen zum Thema

- Authentifizierungsmodule aktivieren auf Seite 101
- Authentifizierungsmodule zu Anwendungen zuweisen auf Seite 101
- Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren auf Seite 102
- Eigenschaften von Authentifizierungsmodulen auf Seite 102
- Initiale Daten für Authentifizierungsmodule auf Seite 103
- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 107

- One Identity Manager Authentifizierungsmodule auf Seite 73
- Steuern von Berechtigungen über Programmfunktionen auf Seite 65

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 102

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.

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 `DialogProductHasAuthentifier`.
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 102

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 101
- Authentifizierungsmodule aktivieren auf Seite 101

Eigenschaften von Authentifizierungsmodulen

Tabelle 32: Eigenschaften von Authentifizierungsmodulen

Eigenschaft	Bedeutung
Aktiviert	Angabe, ob das Authentifizierungsmoduls zur Verwendung aktiviert ist.

Eigenschaft	Bedeutung
Anzeigename	Der Anzeigename wird zur Anzeige des Authentifizierungsmoduls im Anmeldedialog der Administrationswerkzeuge verwendet.
Authentifizierungsmodul	Interner Name des Authentifizierungsmoduls.
Authentifizierungstyp	Legt den Typ des Athentifizierungsmoduls 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.
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 33: Initiale Daten für Authentifizierungsmodule

Anzeigename des Moduls	Authen-tifizierungsmodul	Parameter	Bedeutung/ Anmerkung
Systembenutzer	DialogUser	User	Benutzername.
		Password	Kennwort des Benutzers.
Active Directory Benutzerkonto	ADSAccount		
Active Directory Benutzerkonto (dynamisch)	DynamicADSAccount	Produkt	Anwendung. Der System-benutzer wird über die Konfigurationsdaten der Anwendung bestimmt.
Active Directory Benutzerkonto (manuelle Eingabe)	DynamicManualADS	Produkt	Anwendung. Der System-benutzer 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 Konfi-gurationsparameter **TargetSystem | ADS | Authen-ticationDomains** an.
		Password	Kennwort des Benutzers.
Active Directory Benutzerkonto (rollenbasiert)	RoleBasedADSAccount		Keine Parameter erfor-derlich.
Active Directory Benutzerkonto (manuelle Einga-be/rollenbasiert)	RoleBasedManualADS	User	Benutzername. Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Die

Anzeigename des Moduls	Authen-tifizierungsmodul	Parameter	Bedeutung/ Anmerkung
			zulässigen Active Directory Domänen geben Sie im Konfi-gurationsparameter **TargetSystem | ADS | Authen-ticationDomains** an.
		Password	Kennwort des Benutzers.
Person	Person	User	Zentrales Benutzerkonto der Person.
		Password	Kennwort des Benutzers.
Person (dynamisch)	DynamicPerson	Produkt	Anwendung. Der System-benutzer wird über die Konfigurationsdaten der Anwendung bestimmt.
		User	Benutzername.
		Password	Kennwort des Benutzers.
Person (rollen-basiert)	RoleBasedPerson	User	Benutzername.
		Password	Kennwort des Benutzers.
HTTP Header	HTTPHeader	Header	Zu nutzender HTTP Header.
		KeyColumn	Kommagetrennte Liste der Schlüsselspalten in der Tabelle `Person`, in denen nach dem Benut-zernamen gesucht werden soll. Standard: `CentralAccount, PersonnelNumber`
HTTP Header (rollen-basiert)	RoleBasedHTTPHeader		Zu nutzender HTTP-Header.
		KeyColumn	Kommagetrennte Liste der Schlüsselspalten in Tabelle `Person`, in denen nach dem Benut-zernamen gesucht

Anzeigename des Moduls	Authen-tifizierungsmodul	Parameter	Bedeutung/ Anmerkung
			werden soll. Standard: `CentralAccount, PersonnelNumber`
LDAP Benutzerkonto (dynamisch)	DynamicLdap	User	Benutzername. Standard: `CN, 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 (rollen-basiert)	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.
		SearchCo-lumn	Spalte aus der `SearchTable`, in welcher nach dem Benut-zernamen des angemel-deten 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.

Anzeigename des Moduls	Authen-tifizierungsmodul	Parameter	Bedeutung/ Anmerkung
OAuth 2.0/OpenID Connect	OAuth		Abhängig vom Authen-tifizierungsverfahren des Sicher-heitstokendienstes.
OAuth 2.0/OpenID Connect (rollen-basiert)	OAuthRoleBased		Abhängig vom Authen-tifizierungsverfahren des Sicher-heitstokendienstes.
Kontobasierter Systembenutzer	DialogUserAccountBased		Keine Parameter erfor-derlich.
Benutzerkonto	QERAccount		Keine Parameter erfor-derlich.
Benutzerkonto (rollenbasiert)	RoleBasedQERAccount		Keine Parameter erfor-derlich.
Kennwort-rücksetzung	PasswordReset		Keine Parameter erfor-derlich.
Kennwort-rücksetzung (rollen-basiert)	RoleBasedPasswordRese t		Keine Parameter erfor-derlich.

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 107
- One Identity Manager Authentifizierungsmodule auf Seite 73

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 109
- Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 110
- Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 111
- Erteilen von Berechtigungen auf das One Identity Manager Schema 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**, und passen die Konfigurationsdaten wie folgt an:

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

Legen Sie eine neue Rechtegruppe **WebShop_Customer** 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** auf.

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 107

- Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 110
- Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 111
- Erteilen von Berechtigungen auf das One Identity Manager Schema 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** 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 107
- Beispiel für eine einfache Zuordnung zum Systembenutzer auf Seite 109

- Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 111
- Erteilen von Berechtigungen auf das One Identity Manager Schema 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 107
- Beispiel für eine einfache Zuordnung zum Systembenutzer auf Seite 109
- Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 110
- Erteilen von Berechtigungen auf das One Identity Manager Schema auf Seite 36

Gültigkeit einer Anmeldung überprüfen

Um zu verhindern, dass Benutzer mit ihren bestehenden Verbindungen arbeiten, wenn sie seit ihrer Anmeldung deaktiviert wurden, führt das System Gültigkeitsprüfungen aus.

Die Prüfung erfolgt bei der nächsten rechtebasierten Aktion auf der Verbindung nach einem festgelegten Intervall von 20 Minuten.

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

6

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 113
- OAuth 2.0/OpenID Connect Konfiguration erstellen auf Seite 115
- OAuth 2.0/OpenID Connect Konfiguration an Webanwendungen zuweisen auf Seite 120
- Aktivierende und deaktivierende Spalten für die Ermittlung von Benutzerkonten festlegen auf Seite 121
- OAuth 2.0/OpenID Connect auf Seite 93
- OAuth 2.0/OpenID Connect (rollenbasiert) auf Seite 95

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 Authentifzierungsmodul

fordert eine 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 `QBMIdentityClient`)
    a. Zertifikatstext (`QBMIdentityClient.CertificateText`) .
    b. Subject oder Fingerabdruck aus dem lokalen Speicher (`QBMIdentityClient.CertificateSubject` und `QBMIdentityClient.CertificateThumbPrint`).
    c. Zertifikatsendpunkt (`QBMIdentityClient.CertificateEndpoint`).

    Zusätzlich werden das Subjekt oder der Fingerabdruck verwendet, um Zertifikate vom Server zur prüfen, wenn sie angegeben sind und nicht auf dem Server lokal existieren.
2. Konfiguration des Identitätsanbieters (Tabelle `QBMIdentityProvider`)
    a. Zertifikatstext ((`QBMIdentityProvider.CertificateText`).
    b. Subject oder Fingerabdruck aus dem lokalen Speicher (`QBMIdentityProvider.CertificateSubject` und `QBMIdentityProvider.CertificateThumbPrint`).
    c. Zertifikatsendpunkt (`QBMIdentityProvider.CertificateEndpoint`)).

    Zusätzlich werden das Subjekt oder der Fingerabdruck verwendet, um Zertifikate vom Server zur prüfen, wenn sie angegeben sind und nicht auf dem Server lokal existieren.
    d. JSON-Web-Key-Endpunkt (`QBMIdentityProvider.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 115
- OAuth 2.0/OpenID Connect auf Seite 93
- OAuth 2.0/OpenID Connect (rollenbasiert) auf Seite 95

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 einen Dialogfenster anzeigt. 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 34: Allgemeine Konfigurationsdaten des Identitätsanbieters

Eigenschaft	Beschreibung
Anmeldeendpunkt	Uniform Resource Locator (URL) der erweiterten Anmeldeseite des Sicherheitstokendienstes.

Eigenschaft	Beschreibung
	Beispiel: http://localhost/rsts/login
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 Zertifikatseinstellungen, dann erfassen Sie die Informationen beim Erstellen der Anwendung.

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

Tabelle 35: Informationen zum Zertifikat des Identitätsanbieters

Eigenschaft	Beschreibung
Zertifikatsendpunkt	Uniform Resource Locator (URL) des Zertifikatsendpunkts auf

Eigenschaft	Beschreibung
	dem Autorisierungsserver. Beispiel: https://localhost/RSTS/SigningCertificate
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 36: Ermitteln der Anmeldeinformationen

Eigenschaft	Beschreibung
Wert für die Suche	Kompletter Name des Claim-Typs aus dem beim Identitätsanbieter die Anmeldeinformationen ermittelt werden. Beispiel: Name einer Entität http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier Haben Sie die Konfigurationsdaten automatisch ermittelt, wählen Sie einen Wert aus der Liste.
Spalte für die Suche	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. Beispiel: `ADSAccount.ObjectGUID`
Wert für Benutzernamen	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`). Beispiel: User Principal Name (UPN)

Eigenschaft	Beschreibung
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn Haben Sie die Konfigurationsdaten automatisch ermittelt, wählen Sie einen Wert aus der Liste.

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 37: 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 38: Informationen zum Zertifikat der Anwendung

Eigenschaft	Beschreibung
Zertifikatsendpunkt	Uniform Resource Locator (URL) des Zerti-

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

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

Tabelle 39: Informationen zur Authentifizierungsmethode

Eigenschaft	Beschreibung
Authentifizierungsmethode	Authentifizierungsmethode am Tokenendpunkt. Zulässige Werte sind: • **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 mit privatem Schlüssel .
Privater Schlüssel	Privater Schlüssel als Text, der für die Authentifizierung genutzt wird.

15. Um den Identitätsanbieter und die Anwendung in der One Identity Manager-Datenbank zu erstellen, klicken Sie **Weiter**.
16. 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 115
- Aktivierende und deaktivierende Spalten für die Ermittlung von Benutzerkonten festlegen auf Seite 121

Aktivierende und deaktivierende Spalten für die Ermittlung von Benutzerkonten 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 kennzeichnen oder deaktiviert kennzeichnen.

Es werden 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.

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.

Multifaktor-Authentifizierung im One Identity Manager

Tabelle 40: 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	Der Konfigurationsparameter legt fest, ob die One Identity Hybrid Subscription unterstützt wird. Erweitern Sie den Funktionsumfang von One Identity Manager mit einer One Identity Hybrid Subscription, welche eine Vielzahl zusätzlicher Cloud-Funktionen und -Services bietet. Verwenden Sie die universelle Starling Two-Factor Authentication, um den administrativen Zugriff zu schützen. Erzwingen Sie eine zusätzliche Authentifizierung, wenn Sie einen kritischen Zugriff anfordern oder genehmigen oder um die Out-of-Band Benutzerverifizierung für Kennwortanforderungen zu aktivieren.
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 | ApiKey	Der Konfigurationsparameter enthält den Credential String 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 IdentityStarling Two-Factor Authentication. Dieser Service wird standardmäßig über eine One Identity Hybrid Subscription zur Verfügung gestellt. Sollte Ihr Unternehmen keine One Identity Hybrid Subscription 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 One Identity Hybrid Subscription zu nutzen
     a. Starten Sie das Launchpad.
     b. Wählen Sie **Verbindung zu One Identity Hybrid Subscription** und klicken Sie **Starten**.

        Der Starling Hybrid Konfigurationsassistent wird gestartet.
     c. Folgen Sie den Anweisungen des Starling Hybrid 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 125.
4. (Optional) Legen Sie fest, ob der Sicherheitscode über die Starling 2FA App angefordert werden muss. Weitere Informationen finden Sie unter Sicherheitscode anfordern auf Seite 126.
5. Aktivieren Sie im Manager die Leistungsposition **Neues Starling 2FA Token**.

Weitere Informationen finden Sie unter Bestellung des Starling 2FA Tokens vorbereiten auf Seite 126.

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 Entscheiden von Bestellungen mit Multifaktor-Authentifizierung Attestierung mit Multifaktor-Authentifizierung	One Identity Manager Anwenderhandbuch für das Web Portal

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

1. Wählen Sie im Designer die Kategorie **One Identity Manager Schema**.
2. 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 41: Konfigurationsparameter für die Anforderung des Starling 2FA Sicherheitscodes

Konfigurationsparameter	Bedeutung
QER | Person | Defender | DisableForceParameter QER | Person | Starling | DisableForceParameter	Die Konfigurationsparameter legen fest, ob Starling 2FA gezwungen werden soll, den Sicherheitscode per SMS oder 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 die One Identity Hybrid Subscription 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.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

A

B

D

E

L

M

O

P

R

S

T

Z