One Identity Manager 8.0.3

Administrationshandbuch für Anwendungsrollen

Legende

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

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

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

One Identity Manager Administrationshandbuch für Anwendungsrollen
Aktualisiert - März 2019
Version - 8.0.3

Inhalt

1

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 7
- Inbetriebnahme der Anwendungsrollen auf Seite 25
- Anwendungsrollen bearbeiten auf Seite 26
- Anhang: Rollenbasierte Authentifizierungsmodule auf Seite 36

2

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

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.
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.
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	Beschreibung
	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 | Betriebsunterstützung** zugewiesen werden. Benutzer mit dieser Anwendungsrolle: • Überwachen die Verarbeitung von Prozessen der Jobqueue. • Überwachen die Verarbeitung der DBQueue. • Erstellen Zugangscodes.

Verwandte Themen

- Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen auf Seite 29

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 Complianceregeln vorhanden ist.

Für die Verwaltung von Complianceregeln sind folgende Anwendungsrollen verfügbar.

Tabelle 2: Anwendungsrollen

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.
Ausnahmegenehmiger	Die Ausnahmegenehmiger müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Ausnahmegenehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle:

Anwendungsrolle	Beschreibung
	• 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

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 **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** oder

Anwendungsrolle	Beschreibung
	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

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 Attestierer ermittelt werden.

Anwendungsrolle	Beschreibung
	• 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

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

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.

Anwendungsrolle	Beschreibung
	• Richten bei Bedarf weitere Anwendungsrollen ein.
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

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

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

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.

Anwendungsrolle	Beschreibung
	• Legen fest, nach welchen Entscheidungsverfahren die Entscheider 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

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 sich 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 Zielsystemverantwortliche. Diese Anwendungsrolle stehen zur Verfügung, wenn das Modul für das Zielsystem vorhanden ist. Die Zielsystemverantwortlichen müssen der

Benutzer	Aufgaben
	Anwendungsrolle **Zielsysteme | G Suite** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | SharePoint Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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. • 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

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 unternehmensspezifische Funktionen sind folgende Anwendungsrollen verfügbar.

Tabelle 12: Anwendungsrollen

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. 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.

3

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 ist einmalig auszuführen.

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 28
- Anwendungsrollen bearbeiten auf Seite 26
- Anhang: Rollenbasierte Authentifizierungsmodule auf Seite 36

Anwendungsrollen 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 25.

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

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

Um Anwendungsrollen zu bearbeiten

1. Wählen Sie die Kategorie **One Identity Manager Administration**.
2. Wählen Sie in der Navigationsansicht eine Kategorie aus.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
4. Bearbeiten Sie die Stammdaten der Anwendungsrolle.
5. Speichern Sie die Änderungen.

HINWEIS: Standardanwendungsrollen können nicht gelöscht werden.

Verwandte Themen

- Stammdaten einer Anwendungsrolle auf Seite 27
- Personen an Anwendungsrollen zuweisen auf Seite 28
- Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen auf Seite 29
- Anhang: Rollenbasierte Authentifizierungsmodule auf Seite 36

Stammdaten einer Anwendungsrolle

Wenn Sie neue Anwendungsrollen anlegen, erfassen Sie mindestens Daten in den Pflichteingabefeldern.

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 kundendefinierte Rechtegruppen zuordnen. Weitere Informationen finden Sie unter Unternehmensspezifische Erweiterung der Bearbeitungsrechte von Anwendungsrollen auf Seite 29. 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 Zertifizierungsstatus 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

Eigenschaft	Bedeutung
	durch einen Manager nicht genehmigt.
Vererbung blockieren	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. HINWEIS: Diese Option ist aus Kompatibilitätsgründen zu älteren Programmversionen vorhanden. Es wird empfohlen, die Option nicht zu aktivieren.
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 die Kategorie **One Identity Manager Administration**.
2. Wählen Sie in der Navigationsansicht eine Kategorie.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle.
4. Wählen Sie die Aufgabe **Personen zuweisen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
6. Speichern Sie die Änderungen.

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.

Für die rollenbasierte Anmeldung an den One Identity Manager-Werkzeugen werden verschiedene rollenbasierte Authentifizierungsmodule zur Verfügung gestellt. Bei der Anmeldung einer Person mit einem rollenbasierten Authentifizierungsmodul werden zunächst die Mitgliedschaften der Person in den Anwendungsrollen ermittelt. Über die Zuordnung der Rechtegruppen zu den 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.

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 mit dem Manager und dem 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 die Option **Nur für rollenbasierte Anmeldung**.

2. Stellen Sie Abhängigkeit der neuen Rechtegruppe zur Standardrechtegruppe der Anwendungsrolle her.

   Die Standardrechtegruppe muss dabei als übergeordnete Rechtegruppe zugeordnet werden. Damit vererbt sie ihre Eigenschaften an die neu definierte Rechtegruppe.

3. Vergeben Sie zusätzliche Bearbeitungsrechte auf Menüeinträge, Formulare, Tabellen oder Spalten.
4. Ordnen Sie im Manager die Rechtegruppe der Anwendungsrolle zu.

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

Ausführliche Informationen zum Erstellen von Rechtegruppen und Bearbeiten von Berechtigungen finden Sie im One Identity Manager Konfigurationshandbuch.

Verwandte Themen

- Stammdaten einer Anwendungsrolle auf Seite 27

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.

Dynamische Rolle für eine Anwendungsrolle 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 zu erstellen

1. Wählen Sie die Kategorie **One Identity Manager Administration**.
2. Wählen Sie in der Navigationsansicht eine Kategorie.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle.
4. Wählen Sie die Aufgabe **Dynamische Rolle erstellen**.
5. Erfassen Sie die erforderlichen Stammdaten. Für dynamische Rollen für Anwendungsrollen gelten folgende Besonderheiten:
   - Objektklasse

     "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.

6. Speichern Sie die Änderungen.

Um eine dynamische Rolle zu bearbeiten

1. Wählen Sie die Kategorie **One Identity Manager Administration**.

   In der Navigationsansicht werden die Anwendungsrollen nach Kategorien gruppiert angezeigt. Es werden genau die Anwendungsrollen angezeigt, die Sie entsprechend Ihrer Anwendungsrolle bearbeiten dürfen.
2. Wählen Sie in der Navigationsansicht eine Kategorie.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle.
4. Wählen Sie die Aufgabe **Überblick über die Anwendungsrolle**.
5. Wählen Sie das Formularelement "Dynamische Rollen" und klicken Sie auf die dynamische Rolle.
6. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
7. Bearbeiten Sie die dynamische Rolle.
8. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten einer Anwendungsrolle auf Seite 27

Vererbungsausschluss für Anwendungsrollen festlegen

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 (widersprechende) 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 widersprechende Anwendungsrollen einzusetzen

- Aktivieren Sie im Designer den Konfigurationsparameter "QER\Structures\ExcludeStructures" und kompilieren Sie die Datenbank.

Um widersprechende Anwendungsrollen festzulegen

1. Wählen Sie die Kategorie **One Identity Manager Administration**.
2. Wählen Sie in der Navigationsansicht eine Kategorie.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle, für die Sie widersprechende Anwendungsrollen definieren wollen.
4. Wählen Sie die Aufgabe **Widersprechende Anwendungsrollen bearbeiten**.
5. 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.
6. Speichern Sie die Änderungen.

Abonnierbare Berichte zuweisen

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

Über diese Aufgabe können Sie abonnierbare Berichte an die ausgewählte Anwendungsrolle zuweisen. Alle Personen, die in dieser Anwendungsrolle sind, können die Berichte im Web Portal abonnieren.

HINWEIS: Die Aufgabe ist nur verfügbar, wenn der Anwendungsrolle (oder einer übergeordneten Anwendungsrolle) eine Rechtegruppe zugeordnet ist.

HINWEIS: Abonnierbare Berichte können nicht an die Anwendungsrollen **Basisrollen | Personenverantwortliche**, **Basisrollen | Jeder (Sehen)** und **Basisrollen | Jeder (Ändern)** zugewiesen werden.

1. Wählen Sie die Kategorie **One Identity Manager Administration**.
2. Wählen Sie in der Navigationsansicht eine Kategorie.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle.
4. Wählen Sie die Aufgabe **Abonnierbare Berichte zuweisen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berichte zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Berichte.
6. Speichern Sie die Änderungen.

Ausführliche Informationen zu abonnierbaren Berichten finden Sie im One Identity Manager Administrationshandbuch für Berichtsabonnements.

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.

Um Zusatzeigenschaften für eine Anwendungsrolle festzulegen

1. Wählen Sie die Kategorie **One Identity Manager Administration**.
2. Wählen Sie in der Navigationsansicht eine Kategorie.
3. Wählen Sie in der Ergebnisliste eine Anwendungsrolle.
4. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
6. Speichern Sie die Änderungen.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

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 Rollen, in denen die Personen der ausgewählten Anwendungsrolle ebenfalls Mitglied sind.
Historische Mitgliedschaften anzeigen	Der Bericht listet alle Mitglieder der ausgewählten Anwendungsrolle und den Zeitraum ihrer Mitgliedschaft auf.

Verwandte Themen

- Analyse von Rollenmitgliedschaften und Zuweisungen an Personen auf Seite 34

Analyse von Rollenmitgliedschaften und Zuweisungen an Personen

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

Beispiele

- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzten.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.
- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.

- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 1: Symbolleiste des Berichts "Übersicht aller Zuweisungen"

Tabelle 15: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Anhang: Rollenbasierte Authentifizierungsmodule

WICHTIG: Um die Anwendungsrollen zur Anmeldung zu nutzen, müssen die Benutzer ein rollenbasiertes Authentifizierungsmodul verwenden. Die rollenbasierte Anmeldung ist für den Manager und das Web Portal vorgesehen. Um die rollenbasierte Anmeldung mit anderen One Identity Manager-Werkzeugen zu nutzen, müssen Sie sicherstellen, dass der Benutzer, der durch das Authentifizierungsmodul ermittelt wird, die benötigten Berechtigungen besitzt.

Für die rollenbasierte Anmeldung an den One Identity Manager-Werkzeugen werden verschiedene rollenbasierte Authentifizierungsmodule zur Verfügung gestellt. Bei der Anmeldung einer Person mit einem rollenbasierten Authentifizierungsmodul werden zunächst die Mitgliedschaften der Person in den Anwendungsrollen ermittelt. Über die Zuordnung der Rechtegruppen zu den 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.

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

Folgende rollenbasierten Authentifizierungsmodule sind verfügbar.

Single Sign-on generisch (rollenbasiert)

Anmeldeinformationen	Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzer.
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 16: 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.

Konfigurationsparameter	Bedeutung
	Beispiel: `CN`
QER\Person\GenericAuthenticator\EnabledBy	Der Konfigurationsparameter enthält eine durch Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager-Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung aktiviert.
QER\Person\GenericAuthenticator\DisabledBy	Der Konfigurationsparameter enthält eine durch Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager-Tabelle (SearchTable), die das Benutzerkonto für die Anmeldung deaktiviert. Beispiel: `AccountDisabled`

Person (rollenbasiert)

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 Kennwort 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.

Benutzerkonto (rollenbasiert)

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

Active Directory Benutzerkonto (rollenbasiert)

Anmeldeinformationen	Das Authentifizierungsmodul verwendet die Active Directory Anmeldeinformationen des aktuell an der Arbeitsstation angemeldeten Benutzer.
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/rollenbasiert)

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.

LDAP Benutzerkonto (rollenbasiert)

Anmeldeinformationen	Anmeldenamen, 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 17: 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.

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 (rollenbasiert)

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. 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. Dafür muss der Claim-Typ bekannt sein, dessen Wert zur Kennzeichnung der Datenänderungen verwendet wird.

Das jeweilige Frontend fordert am Authorisierungsendpunkt den Autorisierungscode an. Über den Konfigurationsparameter "QER\Person\OAuthAuthenticator\LoginEndpoint" 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 Konfigurationsparameter verwendet. Um das Zertifikat zur Prüfung der Token zu ermitteln, werden die Zertifikatsspeicher in folgender Reihenfolge abgefragt:

1. Konfiguration der Webanwendung (Tabelle `QBMWebApplication`)
    a. Zertifikatstext (`QBMWebApplication.CertificateText`) .
    b. Subject oder Fingerabdruck aus dem lokalen Speicher (`QBMWebApplication.OAuthCertificateSubject` und `QBMWebApplication.OAuthCertificateThumbPrint`).
    c. Zertifikatsendpunkt (`QBMWebApplication.CertificateEndpoint`).

       Zusätzlich werden das Subject oder der Fingerabdruck verwendet, um Zertifikate vom Server zur prüfen, wenn sie angegeben sind und nicht auf dem Server lokal existieren.
2. Konfigurationsparameter
    a. Zertifikatstext (Konfigurationsparameter "QER\Person\OAuthAuthenticator\CertificateText").
    b. Subject oder Fingerabdruck aus dem lokalen Speicher (Konfigurationsparameter "QER\Person\OAuthAuthenticator\CertificateSubject" und "QER\Person\OAuthAuthenticator\CertificateThumbPrint").
    c. Zertifikatsendpunkt (Konfigurationsparameter "QER\Person\OAuthAuthenticator\CertificateEndpoint").

       Zusätzlich werden das Subject oder der Fingerabdruck verwendet, um Zertifikate vom Server zur prüfen, wenn sie angegeben sind und nicht auf dem Server lokal exisitieren.
    d. JSON-Web-Key-Endpunkt (Konfigurationsparameter "QER\Person\OAuthAuthenticator\JsonWebKeyEndpoint").

Um das Benutzerkonto zu ermitteln, wird der Claim-Typ benötigt, aus dem die Benutzerinformationen ermittelt werden. Zusätzlich wird festgelegt, welche Informationen des One Identity Manager Schemas zur Suche des Benutzerkontos verwendet werden.

Die Authentifizierung über OpenID Connect baut auf OAuth auf. Die OpenID Connect Authentifizierung benutzt dieselben Mechanismen, stellt aber die Benutzer-Claims in einem ID-Token oder über einen User Info Endpunkt zur Verfügung. Für den Einsatz von OpenID Connect sind weitere Konfigurationseinstellungen erforderlich. Ist im Konfigurationsparameter "QER\Person\OAuthAuthenticator\Scope" der Wert "openid" enthalten, verwendet das Authentifizierungsmodul "OpenID Connect".

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

Tabelle 18: Konfigurationsparameter für das Authentifizierungsmodul

Konfi-gurationsparameter	Bedeutung
QER\Per-son\OAuthAuthenticator	Der Konfigurationsparameter legt fest, ob die Authen-tifizierung über Sicherheitstoken unterstützt wird.
QER\Per-	Der Konfigurationsparameter enthält den Uniform Resource

Konfigurationsparameter	Bedeutung
son\OAuthAuthenticator\CertificateEndpoint	Locator (URL) des Zertifikatsendpunkts auf dem Autorisierungsserver. Beispiel: `https://localhost/RSTS/SigningCertificate`
QER\Person\OAuthAuthenticator\CertificateSubject	Der Konfigurationsparameter enthält das Subject des Zertifikats, das zur Überprüfung verwendet wird. Subject oder Fingerabdruck müssen gesetzt sein.
QER\Person\OAuthAuthenticator\CertificateThumbPrint	Der Konfigurationsparameter enthält den Fingerabdruck des zu verwendenden Zertifikates zur Prüfung des Sicherheitstokens.
QER\Person\OAuthAuthenticator\ClientID	Der Konfigurationsparameter legt fest, ob Client-Anwendungen die Authentifizierung unterstützen.
QER\Person\OAuthAuthenticator\ClientID\Web	Der Konfigurationsparameter enthält den Uniform Resource Name (URN) der Web Anwendung, welche die Authentifizierung unterstützt. Beispiel: `urn:OneIdentityManager/Web`
QER\Person\OAuthAuthenticator\ClientID\Windows	Der Konfigurationsparameter enthält Uniform Resource Name (URN) der nativen Anwendung, welche die Authentifizierung unterstützt. Beispiel: `urn:OneIdentityManager/WinClient`
QER\Person\OAuthAuthenticator\DisabledByColumns	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`
QER\Person\OAuthAuthenticator\EnabledByColumns	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\OAuthAuthenticator\IssuerName	Der Konfigurationsparameter enthält den Uniform Resource Name (URN) des Aussteller des Zertifikates zur Prüfung des Sicherheitstokens. Beispiel: `urn:RSTS/identity`
QER\Person\OAuthAuthenticator\LoginEndpoint	Der Konfigurationsparameter enthält den Uniform Resource Locator (URL) der erweiterten Anmeldeseite des Sicherheitstokendienstes. Beispiel: `http://localhost/rsts/login`

Konfigurationsparameter	Bedeutung
QER\Person\OAuthAuthenticator\Resource	Der Konfigurationsparameter enthält den Uniform Resource Name (URN) der abzufragenden Ressource, zum Beispiel für ADFS.
QER\Person\OAuthAuthenticator\SearchClaim	Der Konfigurationsparameter enthält den Uniform Resource Identifier (URI) des Claim-Typs aus dem die Anmeldeinformationen ermittelt werden. Beispiel: Name einer Entität http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
QER\Person\OAuthAuthenticator\SearchColumn	Der Konfigurationsparameter enthält die Spalte aus der One Identity Manager-Tabelle (SearchTable), die zur Suche der Benutzerinformationen verwendet wird. Entsprechung des Claim-Typs (SearchClaim) im One Identity Manager Schema. Beispiel: `ObjectGUID`
QER\Person\OAuthAuthenticator\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\OAuthAuthenticator\TokenEndpoint	Der Konfigurationsparameter enthält den Uniform Resource Locator (URL) des Tokenendpunktes des Autorisierungsservers für die Rückgabe des Zugriffstokens an den Client für die Anmeldung. Beispiel: `https://localhost/rsts/oauth2/token`
QER\Person\OAuthAuthenticator\UserNameClaim	Der Konfigurationsparameter enthält den Uniform Resource Identifier (URI) des Claim-Typs, der verwendet wird, um Datenänderungen zu kennzeichnen (`XUserInserted`, `XUserUpdated`). Beispiel: User Principal Name (UPN) http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
QER\Person\OAuthAuthenticator\InstalledRedirectUri	Der Konfigurationsparameter enthält den Uniform Resource Identifier (URI) zur Weiterleitung für installierte Applikationen. Beispiel: `urn:InstalledApplication`

Konfigurationsparameter	Bedeutung
QER\Person\OAuthAuthenticator\AllowSelfSignedCertsForTLS	Der Konfigurationsparameter legt fest, ob die Nutzung von selbstsignierten Zertifikaten bei der Verbindung zum Token- und User Info Endpunkt erlaubt ist.
QER\Person\OAuthAuthenticator\CertificateText	Der Konfigurationsparameter enthält den Inhalt des Zertifikats als Base64-kodierte Zeichenkette. Es wird nur benutzt, wenn kein Zertifikatsendpunkt konfiguriert ist.
QER\Person\OAuthAuthenticator\JsonWebKeyEndpoint	Der Konfigurationsparameter enthält den URL des JSON-Web-Key-Endpunktes, der die Signierungsschlüssel liefert. Derzeit werden nur JWK-Dateien unterstützt, die die Zertifikate im x5c-Feld (Certificate Chain) enthalten.
QER\Person\OAuthAuthenticator\LogoutEndpoint	Der Konfigurationsparameter enthält den Uniform Resource Locator (URL) des Abmelde-Endpunktes. Beispiel: `http://localhost/rsts/login?wa=wsignout1.0`
QER\Person\OAuthAuthenticator\SharedSecret	Der Konfigurationsparameter enthält den Shared-Secret-Wert, der für die Authentifizierung am Tokenendpunkt genutzt wird.
QER\Person\OAuthAuthenticator\TokenEndpointAuthentication	Der Konfigurationsparameter enthält die beim Tokenendpunkt zu benutzende Authentifizierungsmethode. Sie legt fest, wie das Shared-Secret übergeben wird. 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.

Tabelle 19: Zusätzliche Konfigurationsparameter für OpenID Connect

Konfigurationsparameter	Bedeutung
QER\Person\OAuthAuthenticator\Scope	Der Konfigurationsparameter legt das Protokolls für die Authentifizierung fest. Besitzt der Konfigurationsparameter einen Wert "openid", wird OpenID Connect verwendet, ansonsten OAuth2.
QER\Person\OAuthAuthenticator\UserInfoEndpoint	Der Konfigurationsparameter enthält den Uniform Resource Locator (URL) des OpenID Connect User Info Endpunktes.

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

D

P