One Identity Manager 9.1.3

Handbuch zur Autorisierung und Authentifizierung

One Identity Manager Handbuch zur Autorisierung und Authentifizierung
Aktualisiert - 29. April 2024, 12:20 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

Über dieses Handbuch

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

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

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

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

Verfügbare Dokumentation

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

2

One Identity Manager Anwendungsrollen

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

Anwendungsrollen erfüllen folgende Ziele:

- Programmfunktionen, Personen, Unternehmensressourcen, Genehmigungsabläufe und Entscheidungsverfahren sind festen Anwendungsrollen zugeordnet. Die Berechtigungen dieser Anwendungsrollen müssen nicht unternehmensspezifisch festgelegt werden. Damit wird die Administration von Berechtigungen vereinfacht.
- Es wird eine revisionssichere interne Verwaltung der One Identity Manager Benutzer und ihrer Berechtigungen ermöglicht. Die Vergabe von Berechtigungen erfolgt durch Zuordnung, Bestellung und Genehmigung oder durch die Berechnung aufgrund bestimmter Eigenschaften einer Person. Die Plausibilität der Berechtigungen 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 Berechtigungsgruppen verknüpft werden, deren Berechtigungen durch den One Identity Manager vordefiniert sind. Berechtigungen steuern

- den Zugriff auf Objekte und deren Eigenschaften,
- die Gestaltung der Menüführung in den Administrationswerkzeugen,
- 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 Berechtigungen. 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 10
- Inbetriebnahme der Anwendungsrollen auf Seite 31
- Anwendungsrollen erstellen und bearbeiten auf Seite 32

Verwandte Themen

- Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen auf Seite 43
- One Identity Manager Authentifizierungsmodule auf Seite 80

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.

Detaillierte Informationen zum Thema

- Anwendungsrollen für Basisfunktionen auf Seite 11
- Anwendungsrollen für das Web Portal für Betriebsunterstützung auf Seite 13
- Anwendungsrolle für Compliance & Security Officer auf Seite 14
- Anwendungsrolle für Auditoren auf Seite 15
- Anwendungsrollen für Identity Audit auf Seite 15
- Anwendungsrollen für Unternehmensrichtlinien auf Seite 17
- Anwendungsrollen für Attestierung auf Seite 19
- Anwendungsrolle für abonnierbare Berichte auf Seite 20
- Anwendungsrolle für Führungsebene auf Seite 21
- Anwendungsrollen für Geschäftsrollen auf Seite 21
- Anwendungsrollen für Organisationen auf Seite 22
- Anwendungsrolle für Anwendungsrollen auf Seite 24

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. • Attestieren die Stammdaten von 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.

Anwendungsrolle	Beschreibung
	Soll jedem Benutzer bei der Anmeldung automatisch eine kundendefinierte Berechtigungsgruppe zugewiesen werden, so kann diese Berechtigungsgruppe 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 Berechtigungsgruppe zugewiesen werden, so kann diese Berechtigungsgruppe 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 neue Personen anlegen und die Stammdaten ihrer Mitarbeiter bearbeiten. • Können ihre Mitarbeiter in den IT Shop aufnehmen. • Können im Web Portal die Complianceregelverletzungen ihrer Mitarbeiter sehen. • Können im Web Portal Delegierungen für ihre Mitarbeiter erstellen. • Können im Web Portal die Delegierungen ihrer Mitarbeiter sehen und bearbeiten. Die Mitglieder dieser Anwendungsrolle werden über eine

Anwendungsrolle	Beschreibung
	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.
Selbstregistrierte Personen	Der Anwendungsrolle **Basisrollen | Selbstregistrierte Personen** werden alle neuen, externen Personen zugewiesen, die sich im Web Portal selbst registriert haben. Die Personen werden über eine dynamische Rolle ermittelt.

Verwandte Themen

- Unternehmensspezifische Erweiterung der Berechtigungen von Anwendungsrollen auf Seite 36
- Anwendungsrollen für das Web Portal für Betriebsunterstützung auf Seite 13

Anwendungsrollen für das Web Portal für Betriebsunterstützung

Das Web Portal für Betriebsunterstützung unterstützt Sie bei der Verwaltung und beim Betrieb Ihrer Webanwendungen. Ausführliche Informationen erhalten Sie im *One Identity Manager Web Portal für Betriebsunterstützung Anwenderhandbuch*.

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

Für das Web Portal für Betriebsunterstützung sind die folgenden Anwendungsrollen verfügbar.

Tabelle 2: Anwendungsrollen für das Web Portal für Betriebsunterstützung

Anwendungsrolle	Beschreibung
Betriebsunterstützung	Personen, die das Web Portal für Betriebsunterstützung nutzen, müssen der Anwendungsrolle **Basisrollen** | **Betriebsunterstützung** zugewiesen werden. Die Mitglieder dieser Anwendungsrolle: • Überwachen die Verarbeitung von Prozessen der

Anwendungsrolle	Beschreibung
	Jobqueue. • Überwachen die Verarbeitung der DBQueue. • Erstellen Zugangscodes, um Mitarbeitern zu ermöglichen, sich am Kennwortrücksetzungsportal anzumelden.
Kennwort-Helpdesk	Die Mitglieder der Anwendungsrolle **Basisrollen | Betriebsunterstützung | Kennwort-Helpdesk** können im Web Portal für Betriebsunterstützung Kennwörter für andere Mitarbeiter zurücksetzen.
Nachbehandlung der Synchronisation	Die Mitglieder der Anwendungsrolle **Basisrollen | Betriebsunterstützung | Nachbehandlung der Synchronisation** sind berechtigt im Web Portal für Betriebsunterstützung die Objekte zu managen, die bei der Synchronisation als ausstehend erkannt wurden.
Systemadministratoren	Die Mitglieder der Anwendungsrolle **Basisrollen | Betriebsunterstützung | Systemadministratoren** können im Web Portal für Betriebsunterstützung die Verarbeitung der Jobqueue und die Verarbeitung der DBQueue starten und stoppen.

Anwendungsrolle für Compliance & Security Officer

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

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

Benutzer mit dieser Anwendungsrolle:

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

Anwendungsrolle für 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 3: 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

Anwendungsrolle	Beschreibung
	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: • 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 einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle:

Anwendungsrolle	Beschreibung
	• 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 4: 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 weisen die Richtlinienverantwortlichen zu. • Können bei Bedarf die Berechnung der Richtlinien starten und Richtlinienverletzungen einsehen. • Erstellen Berichte über Richtlinienverletzungen. • Erfassen risikomindernde Maßnahmen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Administrieren die Anwendungsrollen für Richtlinienverantwortliche, Ausnahmegenehmiger und Attestierer.

Anwendungsrolle	Beschreibung
	• 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	Die Ausnahmegenehmiger müssen der Anwendungsrolle **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 Anwendungsrollen stehen zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Für die Verwaltung der Attestierungsverfahren sind folgende Anwendungsrolle verfügbar.

Tabelle 5: 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 Attestierer 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. • Administrieren die Anwendungsrollen für die Eigentümer von Attestierungsrichtlinien. • Pflegen die Mitglieder der zentralen Entscheidergruppe.
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.
Attestierer für externe Benutzer	Die Attestierer für externe Benutzer müssen der Anwendungsrolle **Identity & Access Governance | Attestierung | Attestierer für externe Benutzer** zugewiesen sein.

Anwendungsrolle	Beschreibung
	Benutzer mit dieser Anwendungsrolle: • Attestieren neue externe Personen.
Eigentümer von Attestierungsrichtlinien	Die Eigentümer von Attestierungsrichtlinien müssen einer untergeordneten Anwendungsrolle der Anwendungsrolle **Identity & Access Governance | Attestierung | Eigentümer von Attestierungsrichtlinien** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind inhaltlich verantwortlich und bearbeiten die Attestierungsrichtlinie, der sie zugewiesen sind. • Ordnen das Attestierungsverfahren, die Entscheidungsrichtlinie und den Zeitplan der Berechnung zu. • Weisen Entscheider, risikomindernde Maßnahmen und Compliance Frameworks zu. • Überwachen die Attestierungsvorgänge und Attestierungsläufe.

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

Anwendungsrolle für abonnierbare Berichte

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

Für die Verwaltung von abonnierbaren Berichten ist folgende Anwendungsrolle verfügbar.

Tabelle 6: 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. • Konfigurieren die Berichtsparameter für abonnierbare

Anwendungsrolle	Beschreibung
	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.

Anwendungsrolle für Führungsebene

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

Für die Verwaltung der Geschäftsrollen sind folgende Anwendungsrollen verfügbar.

Tabelle 7: 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. • Attestieren die Stammdaten von Geschäftsrollen. • Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
Zusätzliche Manager	Die zusätzlichen Manager müssen der Anwendungsrolle **Identity**

Anwendungsrolle	Beschreibung
	Management | Geschäftsrollen | Zusätzliche Manager oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind berechtigt Geschäftsrollen zu verwalten.
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 8: 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. • Attestieren die Stammdaten von Abteilungen, Kostenstellen und Standorten. • Administrieren die Anwendungsrollen für Genehmiger, Genehmiger (IT) und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
Zusätzliche Manager	Die zusätzlichen Manager müssen der Anwendungsrolle **Identity Management | Organisationen | Zusätzliche Manager** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind berechtigt Abteilungen, Kostenstellen und Standorte zu verwalten.
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.

Anwendungsrolle	Beschreibung
	• Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.
Genehmiger (IT)	Die IT Genehmiger müssen der Anwendungsrolle **Identity Management | Organisationen | Genehmiger (IT)** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind IT Genehmiger für den IT Shop. • Entscheiden über Bestellungen aus Abteilungen, Kostenstellen und Standorten, für die sie verantwortlich sind.

Anwendungsrolle für Anwendungsrollen

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

Für die Verwaltung der Anwendungsrollen ist folgende Anwendungsrolle verfügbar.

Tabelle 9: Anwendungsrollen für Organisationen

Anwendungsrolle	Beschreibung
Zusätzliche Manager	Die zusätzlichen Manager müssen der Anwendungsrolle **Identity Management | Anwendungsrollen | Zusätzliche Manager** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind berechtigt Anwendungsrollen zu verwalten.

Anwendungsrolle für Personenadministratoren

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

Für die Verwaltung der Personen ist folgende Anwendungsrolle verfügbar.

Tabelle 10: 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 Personen Manager zu. • Weisen Unternehmensressourcen an die Personen zu. • Überprüfen und autorisieren die Stammdaten von Personen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Bearbeiten Kennwortrichtlinien für Kennwörter von Personen. • Können Sicherheitsschlüssel (Webauthn) von Personen löschen. • Können im Web Portal die Bestellungen, Attestierungen und Delegierungen aller Personen sehen und Delegierungen bearbeiten.

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 11: 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 Entscheider ermittelt werden.

Anwendungsrolle	Beschreibung
	• Erstellen die Produkte und Leistungspositionen. • Richten die Benachrichtigungen für Bestellvorgänge ein. • Überwachen die Bestellvorgänge. • Administrieren die Anwendungsrollen für Produkteigner und Attestierer. • Pflegen die Mitglieder der zentralen Entscheidergruppe. • Richten bei Bedarf weitere Anwendungsrollen ein. • Erstellen Zusatzeigenschaften für beliebige Unternehmensressourcen. • Bearbeiten Ressourcen und weisen diese an IT Shop-Strukturen 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. • Attestieren Objekte, denen Leistungspositionen zugeordnet 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 12: Anwendungsrollen für Zielsysteme

Anwendungsrolle	Aufgaben
Administratoren	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 ausschließen. • 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. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem.

Anwendungsrolle	Aufgaben
	• Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
Zielsystemverantwortliche für den Unified Namespace	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 13: Anwendungsrollen für das Universal Cloud Interface

Anwendungsrolle	Aufgaben
Cloud-Administratoren	Die Cloud-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 Cloud-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 Cloud-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.

Anwendungsrolle für Privileged Account Governance

HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Privileged Account Governance Modul vorhanden ist.

Für die Verwaltung der Asset- und Konteneigentümer ist folgende Anwendungsrolle verfügbar.

Tabelle 14: Anwendungsrollen für Privileged Account Governance

Anwendungsrolle	Beschreibung
Asset- und Konteneigentümer	Die Eigentümer privilegierter Objekte wie PAM Assets, PAM Assetkonten, PAM Verzeichniskonten, PAM Assetgruppen und PAM Kontogruppen müssen einer Anwendungsrolle unter der Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über die Bestellung von Zugriffsanforderungen für privilegierte Objekte. • Attestieren den möglichen Zugriff von Benutzern auf diese privilegierten Objekte.

Anwendungsrollen für Application Governance

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

Tabelle 15: Anwendungsrollen für Application Governance

Anwendungsrolle	Aufgaben
Administratoren	Die Administratoren müssen der Anwendungsrolle **Application Governance | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen im Web Portal neue Geschäftsanwendungen. • Verwalten im Web Portal sämtliche Geschäftsanwendungen.
Eigentümer	Die Eigentümer von Geschäftsanwendungen müssen der Anwendungsrolle **Application Governance | Eigentümer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Können im Web Portal Geschäftsanwendungen bearbeiten, für die sie verantwortlich sind.
Entscheider	Die Entscheider müssen der Anwendungsrolle **Application Governance | Entscheider** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über die Bestellungen von Produkten der Geschäftsanwendungen.

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 16: 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 Berechtigungen auf kundenspezifische Tabellen oder Spalten zu gewähren. Alle Anwendungsrollen, die Sie hier definieren, müssen ihre Berechtigungen über kundendefinierte Berechtigungsgruppen 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**.

   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.

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.

Verwandte Themen

- Personen an Anwendungsrollen zuweisen auf Seite 35
- Anwendungsrollen erstellen und bearbeiten auf Seite 32

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 31.

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 33
- Personen an Anwendungsrollen zuweisen auf Seite 35
- Unternehmensspezifische Erweiterung der Berechtigungen von Anwendungsrollen auf Seite 36
- Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten auf Seite 37
- One Identity Manager Authentifizierungsmodule auf Seite 80

Stammdaten von Anwendungsrollen

Tabelle 17: 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

Eigenschaft	Bedeutung
	Information. Sie sagen nichts darüber aus, für welche Abteilung, Kostenstelle oder Standort die Anwendungsrollen zuständig sind.
Manager	Verantwortlicher Manager der Anwendungsrolle.
2. Verantwortlicher	Stellvertretender Manager der Anwendungsrolle.
Zusätzliche Manager	Anwendungsrolle für eine Gruppe von Managern und Stellvertretern, die diese Anwendungsrolle verwalten. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Berechtigungsgruppe	Berechtigungsgruppe für die Ermittlung der Berechtigungen bei rollenbasierter Anmeldung. Eine Anwendungsrolle erhält die Berechtigungen der zugeordneten Berechtigungsgruppe. Ist keine Berechtigungsgruppe zugeordnet, erhält die Anwendungsrolle die Berechtigungen der übergeordneten Anwendungsrolle. Administratoren können den übrigen Anwendungsrollen kundendefinierte Berechtigungsgruppen zuordnen. HINWEIS: Die Berechtigungsgruppen 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. Der Zertifizierungsstatus kann abhängig vom Ergebnis regelmäßiger Attestierungen gesetzt werden.
Vererbung blockieren	Gibt an, ob die Vererbung an dieser Anwendungsrolle unterbrochen wird. Aktivieren Sie diese Option, um die Vererbung von Unternehmensressourcen an untergeordnete Anwendungsrollen zu verhindern.

Eigenschaft	Bedeutung
	HINWEIS: Die Unterbrechung der Vererbung für Anwendungsrollen ist nur für kundendefinierte Anwendungsrollen zulässig.
Dynamische Rollen nicht erlaubt	Gibt an, 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.

Verwandte Themen

- Anwendungsrolle für Anwendungsrollen auf Seite 24
- Unternehmensspezifische Erweiterung der Berechtigungen von Anwendungsrollen auf Seite 36
- Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten auf Seite 37
- Zertifizierung von Anwendungsrollen auf Seite 40

Personen an Anwendungsrollen zuweisen

Die zugewiesenen Personen erhalten alle Berechtigungen der Berechtigungsgruppe, 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 erhalten die Personen der übergeordneten Anwendungsrolle die Berechtigungen.

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

Um Personen an eine Anwendungsrolle zuzuweisen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

4. Speichern Sie die Änderungen.

Verwandte Themen

- Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten auf Seite 37

Unternehmensspezifische Erweiterung der Berechtigungen von Anwendungsrollen

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

Einigen der Standardanwendungsrollen sind bereits Berechtigungsgruppen zugewiesen. Diese Berechtigungsgruppen besitzen die Berechtigungen 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 Berechtigungen der Anwendungsrollen Ihren unternehmensspezifischen Erfordernissen anzupassen, können Sie den Anwendungsrollen kundendefinierte Berechtigungsgruppen zuordnen. Damit Benutzer mit diesen Anwendungsrollen alle Funktionen des One Identity Manager wie in der Standardinstallation nutzen können, sorgen Sie dafür, dass Ihre kundendefinierten Berechtigungsgruppen alle Berechtigungen der Standardberechtigungsgruppen dieser Anwendungsrollen erhalten.

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

Gehen Sie folgendermaßen vor:

1. Erstellen Sie im Designer eine neue Berechtigungsgruppe.

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

2. Stellen Sie im Designer die Abhängigkeit der neuen Berechtigungsgruppe zur Standardberechtigungsgruppe der Anwendungsrolle her. Weisen Sie die Standardberechtigungsgruppe als übergeordnete Berechtigungsgruppe zu. Damit vererbt die Standardberechtigungsgruppe ihre Eigenschaften an die neu definierte Berechtigungsgruppe.
3. Vergeben Sie im Designer zusätzliche Berechtigungen auf Menüeinträge, Formulare, Tabellen oder Spalten.
4. Ordnen Sie im Manager die neue Berechtigungsgruppe der Anwendungsrolle zu.

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

Verwandte Themen

- Stammdaten von Anwendungsrollen auf Seite 33
- Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen auf Seite 43

Dynamische Rollen für Anwendungsrollen erstellen und bearbeiten

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

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

Um eine dynamische Rolle für eine Anwendungsrolle zu erstellen

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

Um eine dynamische Rolle zu bearbeiten

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

5. Bearbeiten Sie die dynamische Rolle.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Anwendungsrollen auf Seite 33

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 Berechtigungsgruppe zugeordnet ist.
- Abonnierbare Berichte können nicht an die Anwendungsrollen **Basisrollen | Personenverantwortliche**, **Basisrollen | Jeder (Sehen)** und **Basisrollen | Jeder (Ändern)** zugewiesen werden.

Um abonnierbare Berichte an einen Anwendungsrolle zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Bericht und doppelklicken Sie .
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 die Schritte zum Erstellen der Zuweisungsressource führt.

Zertifizierung von Anwendungsrollen

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

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

Um den Zertifizierungsstatus einer Anwendungsrolle manuell zu ändern

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

Um den Zertifizierungsstatus von Anwendungsrollen durch Attestierungen zu ändern

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

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

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

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

Detaillierte Informationen zum Thema

- Anwendungsrollen erstellen und bearbeiten auf Seite 32
- Stammdaten von Anwendungsrollen auf Seite 33

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 18: 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

Bericht	Beschreibung
	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.

3

Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen

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

Berechtigungsgruppen 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 Berechtigungsgruppen 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 Berechtigungsgruppen und Systembenutzer mit einer vordefinierten Benutzeroberfläche und Berechtigungen 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

Verwandte Themen

- One Identity Manager Anwendungsrollen auf Seite 9
- One Identity Manager Authentifizierungsmodule auf Seite 80

Vordefinierte Berechtigungsgruppen und Systembenutzer

Der One Identity Manager stellt Berechtigungsgruppen und Systembenutzer mit einer vordefinierten Benutzeroberfläche und speziellen Berechtigungen 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 19: Vordefinierte Berechtigungsgruppen

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

Berechtigungsgruppe	Beschreibung
Berechtigungsgruppen für One Identity Manager-Anwendungsdaten	Die Berechtigungsgruppen besitzen Berechtigungen auf die Tabellen und die Spalten, die Anwendungsdaten abbilden. Diese Berechtigungsgruppen sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um die Anwendungsdaten beispielsweise mit dem Manager zu bearbeiten.
Berechtigungsgruppen für One Identity Manager-Systemdaten	Die Berechtigungsgruppen besitzen die Berechtigungen auf die Tabellen und die Spalten, die Systemdaten des One Identity Manager abbilden. Diese Berechtigungsgruppen sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um Systemdaten zu bearbeiten, beispielsweise mit den Editoren des Designer. Die Berechtigungsgruppe **vid** besitzt alle Berechtigungen für die Systemkonfiguration mit dem Designer.
Rollenbasierte Berechtigungsgruppe **VI_4_ALLUSER**	Die Berechtigungsgruppe **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 Berechtigungsgruppe ist implizit immer zugewiesen.
Rollenbasierte Berechtigungsgruppe **vi_4_ADMIN_LOOKUP**	Die Berechtigungsgruppe **vi_4_ADMIN_LOOKUP** besitzt die Sichtbarkeitsberechtigungen auf alle Tabellen und Spalten, die Anwendungsdaten abbilden. HINWEIS: Weisen Sie der Berechtigungsgruppe die Sichtbarkeitsberechtigungen auf kundenspezifischen Schemaerweiterungen zu.
Rollenbasierte Berechtigungsgruppe **QER_OperationsSupport**	Die Berechtigungsgruppe **QER_OperationsSupport** besitzt spezielle Berechtigungen für die Arbeit mit dem Web Portal für Betriebsunterstützung. Die Berechtigungsgruppe ist der Anwendung **OperationsSupportWebPortal** zugewiesen. Die Berechtigungen der Berechtigungsgruppe gelten nur im Web Portal für Betriebsunterstützung.
Rollenbasierte Berechtigungsgruppen	Rollenbasierte Berechtigungsgruppen besitzen Berechtigungen auf die Tabellen und Spalten, die Anwendungsdaten abbilden. Diese Berechtigungsgruppen sind mit Menüeinträgen, Formularen, Methoden und Programmfunktionen ausgestattet, um mit dem Manager und dem Web Portal die Anwendungsdaten zu bearbeiten. Diese Berechtigungsgruppen sind mit One Identity Manager Anwendungsrollen verknüpft und vereinfachen im One Identity Manager Rollenmodell die Administration der Berechtigungen.

Tabelle 20: 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 Berechtigungsgruppen zu One Identity Manager Anwendungsrollen wird bestimmt, welche Berechtigungsgruppen für die Person gültig sind. Aus diesen Berechtigungsgruppen 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 Berechtigungsgruppe zugeordnet, besitzt jedoch alle Berechtigungen, 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. 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 Berechtigungsgruppen. 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.

Verwandte Themen

- Abhängigkeiten zwischen Berechtigungsgruppen auf Seite 50
- Bearbeitung von Berechtigungsgruppen auf Seite 49

- Systembenutzer erstellen auf Seite 56
- Dynamische Systembenutzer auf Seite 61

Regeln für die Ermittlung der gültigen Berechtigungen für Tabellen und Spalten

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

- Die Berechtigungen hierarchischer Berechtigungsgruppen werden von oben nach unten vererbt. Das heißt, eine Berechtigungsgruppe erhält alle Berechtigungen ihrer übergeordneten Berechtigungsgruppen.
- Bei hierarchischer Berechtigungsgruppen wird zuerst die Menge der Objekte ermittelt. Anschließend werden die Spaltenberechtigungen zusammengefasst. Damit ergeben sich unter Umständen mehr effektive Berechtigungen als auf den einzelnen Berechtigungsgruppen definiert sind.
- Ein Systembenutzer erhält ein Berechtigung, wenn mindestens eine seiner Berechtigungsgruppen das Berechtigung besitzt (direkt oder geerbt).
- Die einschränkenden Bedingungen aller Berechtigungsgruppen des Systembenutzers werden zusammengefasst und somit eine gültige Bedingung pro Berechtigung zum Anzeigen, Bearbeiten, Einfügen und Löschen eines Objektes ermittelt.
- Durch das System werden fest definierte Sichtbarkeitsberechtigungen auf die Systemdaten des One Identity Manager Schemas vergeben, die für die Anmeldung eines Systembenutzers an den Administrationswerkzeugen ausreichend sind.
- Ein Systembenutzer, der nur Leseberechtigungen besitzt, erhält unabhängig von weiteren Berechtigungen nur die Sichtbarkeitsberechtigungen auf die Objekte.
- Werden auf eine Tabelle die Berechtigungen zum Einfügen, Bearbeiten oder Löschen vergeben, werden implizit auch Sichtbarkeitsberechtigungen vergeben.
- Werden auf eine Spalte die Berechtigungen zum Einfügen oder Bearbeiten vergeben, werden implizit die Sichtbarkeitsberechtigungen vergeben.
- Werden Berechtigungen auf eine Tabelle vergeben, so werden implizit Sichtbarkeitsberechtigungen auf die Primärschlüsselspalte der Tabelle vergeben.
- Ist mindestens die Sichtbarkeitsberechtigung auf eine Fremdschlüsselspalte vergeben, so werden implizit Sichtbarkeitsberechtigungen auf die referenzierte Tabelle, auf die Primärschlüsselspalte und die Spalten, die laut definiertem Anzeigemuster an der referenzierten Tabelle zur Anzeige benötigt werden, vergeben.
- Spalten, die im definiertem Anzeigemuster an der Tabelle zur Anzeige benötigt werden, erhalten implizit Sichtbarkeitsberechtigungen.

- Berechtigungen für Datenbanksichten vom Typ **Proxy** gelten auch für die zugrunde liegenden Tabellen.
- Für Datenbanksichten vom Typ **ReadOnly** gelten unabhängig von weiteren Berechtigungen nur die Sichtbarkeitsberechtigungen.
- Ist eine Tabelle oder Spalte durch Präprozessorbedingungen deaktiviert, werden keine Berechtigungen auf diese Tabellen und Spalten ermittelt; die Tabelle oder Spalte gilt als nicht vorhanden.
- Ist eine Berechtigungsgruppe durch Präprozessorbedingungen deaktiviert, werden Berechtigungen dieser Berechtigungsgruppe nicht berücksichtigt; die Berechtigungsgruppe gilt als nicht vorhanden.

Beispiel: Zusammensetzung der Berechtigungen über Berechtigungsgruppen

Nachfolgendes Beispiel zeigt die Zusammensetzung der Berechtigungen, wenn der Benutzer in den Berechtigungsgruppen direkt zugeordnet ist und keine hierarchische Verbindung der Berechtigungsgruppen besteht.

Ein Systembenutzer erhält über verschiedene Berechtigungsgruppen die Berechtigungen auf die Tabelle `ADSAccount`.

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

Zusätzlich erhält er über diese Berechtigungsgruppen Berechtigungen auf die Tabelle `LDAPAccount`.

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

Somit hat der Systembenutzer effektiv folgende Berechtigungen:

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

Beispiel: Einschränkende Bedingungen

Ein Systembenutzer erhält über verschiedene Berechtigungsgruppen Sichtbarkeitsberechtigungen auf die Tabelle `Person`.

Berechtigungsgruppe	Bedingung für Sichtbarkeit	Sichtbarkeit 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
Dreyer	Lastname

Bearbeitung von Berechtigungsgruppen

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

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

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

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

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

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

Folgende Aufgaben können Sie ausführen:

- Stammdaten der Berechtigungsgruppen bearbeiten
- Neue Abhängigkeiten zwischen Berechtigungsgruppen definieren
- Berechtigungsgruppen kopieren
- Neue Berechtigungsgruppen erstellen

Verwandte Themen

- Vordefinierte Berechtigungsgruppen und Systembenutzer auf Seite 44
- Abhängigkeiten zwischen Berechtigungsgruppen bearbeiten auf Seite 51
- Berechtigungsgruppen kopieren auf Seite 53
- Berechtigungsgruppen erstellen auf Seite 54
- Eigenschaften von Berechtigungsgruppen auf Seite 55
- Steuern von Berechtigungen über Programmfunktionen auf Seite 73

Abhängigkeiten zwischen Berechtigungsgruppen

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

Für die Abhängigkeit von Berechtigungsgruppen gilt:

- Eine rollenbasierte Berechtigungsgruppe kann von rollenbasierten Berechtigungsgruppen und nicht-rollenbasierten Berechtigungsgruppen erben.
- Eine nicht-rollenbasierte Berechtigungsgruppe kann von nicht-rollenbasierten Berechtigungsgruppen erben. Eine nicht-rollenbasierte Berechtigungsgruppe darf nicht von rollenbasierten Berechtigungsgruppen erben.

Beispiel:

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

Berechtigungsgruppe	Berechtigungen	Benutzeroberfläche
A	Sichtbar	Menüstruktur und Formulare
B	Bearbeitbar	Methodendefinitionen

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

Verwandte Themen

- Abhängigkeiten zwischen Berechtigungsgruppen bearbeiten auf Seite 51

Abhängigkeiten zwischen Berechtigungsgruppen bearbeiten

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

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

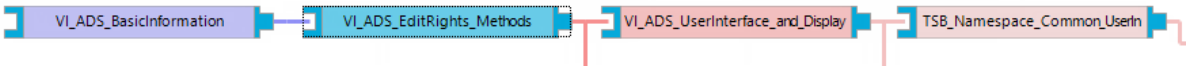

Tabelle 21: Bedeutung der Farben in der hierarchischen Darstellung

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

Um Abhängigkeiten einer Berechtigungsgruppe festzulegen

1. Wählen Sie im Designer die Kategorie **Berechtigungen > Berechtigungsgruppen**.
2. Wählen Sie die Berechtigungsgruppe und starten Sie den Benutzer-& Berechtigungsgruppeneditor über die Aufgabe **Berechtigungsgruppe bearbeiten**.
3. In der hierarchischen Ansicht der Berechtigungsgruppen wählen Sie die Berechtigungsgruppe und führen Sie eine der folgenden Aktionen aus.
   - Wählen Sie das Kontextmenü **Berechtigungen erben von** und wählen Sie die Berechtigungsgruppen, von denen die ausgewählte Berechtigungsgruppe erben soll.
   - Wählen Sie das Kontextmenü **Berechtigungen vererben an** und wählen Sie die Berechtigungsgruppen, die in die ausgewählte Berechtigungsgruppe aufgenommen werden sollen. Die ausgewählte Berechtigungsgruppe vererbt ihre Berechtigung an die untergeordneten Berechtigungsgruppen.
4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Berechtigungsgruppen kopieren

Der Benutzer-& Berechtigungsgruppeneditor stellt einen Assistenten zur Verfügung, um die Berechtigungen und die Benutzeroberfläche einer bestehenden Berechtigungsgruppe auf eine neue Berechtigungsgruppe kopieren.

Um eine Berechtigungsgruppe zu kopieren

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

Tabelle 22: Kopieroptionen für Berechtigungsgruppen

Option	Beschreibung
Berechtigungen	Aktivieren Sie diese Option, um die Tabellenberechtigungen und die Spaltenberechtigungen der gewählten Berechtigungsgruppe auf die neue Berechtigungsgruppe zu kopieren.
Benutzeroberfläche	Aktivieren Sie diese Option, um die Menüeinträge, die Formulare und die Methodendefinitionen der gewählten Berechtigungsgruppe auf die neue Berechtigungsgruppe zu kopieren.
Systembenutzer	Aktivieren Sie diese Option, um die Systembenutzer der gewählten Berechtigungsgruppe in die neue Berechtigungsgruppe aufzunehmen.

Option	Beschreibung
	HINWEIS: Beachten Sie hierbei, dass vordefinierte Systembenutzer nicht in die neue Berechtigungsgruppe 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 Berechtigungsgruppe** 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

- Berechtigungsgruppen erstellen auf Seite 54
- Eigenschaften von Berechtigungsgruppen auf Seite 55
- Abhängigkeiten zwischen Berechtigungsgruppen bearbeiten auf Seite 51
- Systembenutzer in Berechtigungsgruppen aufnehmen auf Seite 59
- Berechtigungen für Tabellen und Spalten auf Seite 61

Berechtigungsgruppen erstellen

Um eine Berechtigungsgruppe zu erstellen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Benutzer-& Berechtigungsgruppeneditor über die Aufgabe **Berechtigungsgruppe anzeigen/bearbeiten**.
3. Fügen Sie eine neue Berechtigungsgruppe über das Menü **Berechtigungsgruppen > Neu** ein.
4. Bearbeiten Sie die Stammdaten der Berechtigungsgruppe.
5. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Berechtigungsgruppen kopieren auf Seite 53
- Eigenschaften von Berechtigungsgruppen auf Seite 55
- Abhängigkeiten zwischen Berechtigungsgruppen bearbeiten auf Seite 51
- Systembenutzer in Berechtigungsgruppen aufnehmen auf Seite 59

Eigenschaften von Berechtigungsgruppen

Tabelle 23: Eigenschaften einer Berechtigungsgruppe

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

- Berechtigungsgruppen kopieren auf Seite 53
- Berechtigungsgruppen erstellen auf Seite 54

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 Berechtigungsgruppen auf und erteilen Sie den Systembenutzern somit Berechtigungen auf die Tabellen und die Spalten des One Identity Manager Schemas 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 Berechtigungsgruppen 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 Berechtigungsgruppen, die den einzelnen Systembenutzern zugewiesen sind. Systembenutzer erstellen und bearbeiten Sie im Designer mit dem Benutzer-& Berechtigungsgruppeneditor.

Folgende Aufgaben können Sie ausführen:

- Neue Systembenutzer erstellen, beispielsweise administrative Systembenutzer oder Systembenutzer für Dienstkonten
- Kennworteinstellungen für Systembenutzer konfigurieren
- Systembenutzer in Berechtigungsgruppen aufnehmen
- Ermitteln, welche Personen einen Systembenutzer verwenden

Verwandte Themen

- Vordefinierte Berechtigungsgruppen und Systembenutzer auf Seite 44
- Systembenutzer erstellen auf Seite 56
- Kennwörter von Systembenutzern auf Seite 57
- Eigenschaften von Systembenutzern auf Seite 58
- Systembenutzer in Berechtigungsgruppen aufnehmen auf Seite 59
- Welche Personen verwenden den Systembenutzer? auf Seite 60
- Dynamische Systembenutzer auf Seite 61

Systembenutzer erstellen

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

Um einen Systembenutzer zu erstellen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Benutzer-& Berechtigungsgruppeneditor über die Aufgabe **Berechtigungsgruppe 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 Berechtigungsgruppen auf.

6. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Vordefinierte Berechtigungsgruppen und Systembenutzer auf Seite 44
- Kennwörter von Systembenutzern auf Seite 57
- Eigenschaften von Systembenutzern auf Seite 58
- Systembenutzer in Berechtigungsgruppen aufnehmen auf Seite 59
- Dynamische Systembenutzer auf Seite 61
- Welche Personen verwenden den Systembenutzer? auf Seite 60
- One Identity Manager Authentifizierungsmodule auf Seite 80

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 58

Eigenschaften von Systembenutzern

Tabelle 24: Eigenschaften eines Systembenutzers

Eigenschaft	Beschreibung
Systembenutzer	Name des Systembenutzers zur Anmeldung an den Administrationswerkzeugen.
Kennwort und Kennwortbestätigung	Kennwort, mit dem sich der Systembenutzer an den Administrationswerkzeugen anmeldet.
Letzte Kennwortänderung	Zeitpunkt der letzten Kennwortänderung.
Kennwort läuft nie ab	Gibt an, ob das Kennwort nie abläuft. Aktivieren Sie die Option beispielsweise für Dienstkonten, um zu verhindern, dass das Kennwort abläuft. Die Option überschreibt das maximale Kennwortalter.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Nur Leseberechtigungen	Setzen Sie die Option, wenn ein Systembenutzer in mehreren Berechtigungsgruppen Mitglied ist, jedoch nur Berechtigungen zum Lesen auf die Objekte haben soll. Damit werden alle Änderungsberechtigungen, die der Systembenutzer über Mitgliedschaften in Berechtigungsgruppen 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	Gibt an, ob es sich um einen administrativen Systembenutzer handelt. Administrative Systembenutzer werden automatisch in alle nicht-rollenbasierten Berechtigungsgruppen aufgenommen. HINWEIS: Einen administrativen Systembenutzer können Sie im Designer im Benutzer-& Berechtigungsgruppeneditor über das Menü **Administrativen Benutzer anlegen** erstellen.
Dienstkonto	Gibt an, ob es sich um einen Systembenutzer handelt, der von einem Dienstkonto verwendet wird. Der Systembenutzer ist keiner Berechtigungsgruppe zugeordnet, besitzt jedoch alle Berechtigungen, Methoden und Programmfunktionen.
Externe Kennwortverwaltung	Gibt an, ob das Kennwort des Systembenutzers über ein externes Kennwortverwaltungssystem ermittelt wird. Das Kennwort kann nicht im One Identity Manager geändert werden.

Eigenschaft	Beschreibung
	Die Ermittlung des Kennwortes für den Systembenutzer muss kundenspezifisch implementiert werden.
Für direkte Anmeldung gesperrt	Gibt an, ob der Systembenutzer für die direkte Anmeldung genutzt werden kann. Aktivieren Sie die Option beispielsweise für Systembenutzer, die für dynamische Authentifizierungsmodule verwendet werden, um eine direkte Anmeldung an den One Identity Manager-Werkzeugen zu verhindern.

Verwandte Themen

- Systembenutzer erstellen auf Seite 56
- Kennwörter von Systembenutzern auf Seite 57
- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 125

Systembenutzer in Berechtigungsgruppen aufnehmen

Nehmen Sie Systembenutzer in Berechtigungsgruppen auf und erteilen Sie somit Berechtigungen auf die Tabellen und die Spalten des One Identity Manager Schemas und stellen die Benutzeroberfläche zur Verfügung.

HINWEIS:

- Systembenutzer können Sie nicht in rollenbasierte Berechtigungsgruppen aufnehmen. Für die rollenbasierte Anmeldung werden dynamische Systembenutzer errechnet.
- Administrative Systembenutzer werden automatisch in alle nicht-rollenbasierten Berechtigungsgruppen aufgenommen.
- Die Berechtigungsgruppe **QBM_BaseRights** definiert die Basisberechtigungen, die für die Anmeldung eines Systembenutzers an den One Identity Manager-Werkzeugen erforderlich sind. Diese Berechtigungsgruppe 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 Berechtigungsgruppen.

Die Mitgliedschaften eines Systembenutzers in Berechtigungsgruppen werden im Designer im Benutzer-& Berechtigungsgruppeneditor dargestellt. Über das Menü **Optionen > Berechtigungsgruppenvererbung** können Sie festlegen, ob die direkten und die

vererbten Mitgliedschaften in Berechtigungsgruppen für einen Systembenutzer angezeigt werden.

Abbildung 2: Mitgliedschaften in Berechtigungsgruppen eines Systembenutzers

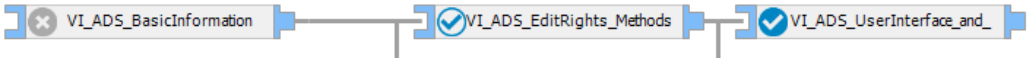

Tabelle 25: Bedeutung der Symbole in der hierarchischen Darstellung

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

Um einen Systembenutzer an eine Berechtigungsgruppe zuzuweisen

1. Wählen Sie im Designer die Kategorie **Berechtigungen > Systembenutzer**.
2. Wählen Sie den Systembenutzer und starten Sie den Benutzer-& Berechtigungsgruppeneditor über die Aufgabe **Systembenutzer bearbeiten**.
3. Wählen Sie in der hierarchischen Ansicht die Berechtigungsgruppe. Per Mausklick auf das Symbol können Sie den ausgewählten Systembenutzer in die Berechtigungsgruppe aufnehmen oder aus der Berechtigungsgruppe entfernen.
4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

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

Verwandte Themen

- Dynamische Systembenutzer auf Seite 61

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-& Berechtigungsgruppeneditor 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

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 Berechtigungsgruppen zu One Identity Manager Anwendungsrollen wird bestimmt, welche Berechtigungsgruppen für die Person gültig sind. Aus diesen Berechtigungsgruppen wird ein dynamischer Systembenutzer berechnet, der für die Anmeldung der Person benutzt wird.

HINWEIS: Dynamische Systembenutzer können Sie nicht bearbeiten. 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 dynamische Systembenutzer, deren Aufbewahrungszeit abgelaufen sind, im Rahmen der täglichen Wartungsaufträge aus der Datenbank gelöscht.

Berechtigungen für Tabellen und Spalten

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

Mit dem Berechtigungseditor können Sie:

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

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

Bei der kundenspezifischen Schemaerweiterungen mit dem Programm Schema Extension legen Sie bereits Berechtigungsgruppen fest. Eine Berechtigungsgruppe erhält Leseberechtigungen und Schreibberechtigungen und eine Berechtigungsgruppe erhält nur Leseberechtigungen. Damit ist ein erster Zugriff auf die kundenspezifischen 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 47
- Berechtigungen von Berechtigungsgruppen anzeigen auf Seite 62
- Berechtigungen für Tabellen anzeigen auf Seite 63
- Tabellenberechtigungen bearbeiten auf Seite 64
- Spaltenberechtigungen bearbeiten auf Seite 66
- Tabellenberechtigungen und Spaltenberechtigungen kopieren auf Seite 67
- Berechtigungen für Systembenutzer simulieren auf Seite 68

Berechtigungen von Berechtigungsgruppen anzeigen

Um alle Berechtigungen für eine Berechtigungsgruppe anzuzeigen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Berechtigungseditor über die Aufgabe **Berechtigungen bearbeiten**.
3. Wählen Sie in der Symbolleiste des Berechtigungseditors in der Auswahlliste **Berechtigungsgruppe** die Berechtigungsgruppe, für die Sie die Berechtigungen anzeigen möchten.

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

- Um Tabellen mit Berechtigungen zuerst anzuzeigen, aktivieren Sie das Menü **Optionen > Berechtigungen** 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 Berechtigungen** im Berechtigungseditor werden die Berechtigungsgruppe angezeigt, die Berechtigungen auf eine Tabelle oder eine Spalte besitzen. Die Berechtigungen sind in dieser Ansicht nicht bearbeitbar.

HINWEIS: Um die Ansicht **Zusammenfassung aller definierten Berechtigungen** anzuzeigen, aktivieren Sie im Berechtigungseditor das Menü **Ansicht > Objektberechtigungen**. Die Ansicht wird im unteren Bereich des Berechtigungseditors angezeigt.

Um alle Berechtigungen für eine Tabelle und ihre Spalten anzuzeigen

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

   In der Ansicht **Zusammenfassung aller definierten Berechtigungen** werden die Berechtigungsgruppe angezeigt, die Berechtigungen 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 Berechtigungen anzuzeigen, öffnen Sie im oberen Bereich des Berechtigungseditors den Eintrag für die Tabelle und wählen Sie eine Spalte.

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

Tabellenberechtigungen bearbeiten

Über die Tabellenberechtigungen 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 Berechtigungen werden im Berechtigungseditor immer für die Berechtigungsgruppe bearbeitet, die Sie in der Symbolleiste des Berechtigungseditors in der Auswahlliste **Berechtigungsgruppe** gewählt haben. Wenn Sie Berechtigungen für eine weitere Berechtigungsgruppe vergeben möchten, wählen Sie diese Berechtigungsgruppe zuerst in der Auswahlliste aus und bearbeiten dann die Berechtigungen.

Um für eine Berechtigungsgruppe die Berechtigungen auf eine Tabelle zu bearbeiten

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

   TIPP: Mit **Umschalt + Auswahl** oder **Strg +Auswahl** können Sie mehrere Tabellen auswählen.
5. Bearbeiten Sie im Bereich **Berechtigungen** die Berechtigungen für die Berechtigungsgruppe.
   - Um neue Berechtigungen einzufügen, wählen Sie das Kontextmenü **Neu** und aktivieren Sie die zugehörigen Kontrollkästchen. Folgende Berechtigungen können Sie vergeben.
     - **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 Berechtigungen **Einfügbar**, **Bearbeitbar** oder **Löschbar** vergeben, wird auch die Berechtigung **Sichtbar** vergeben.
   - Um eine Berechtigung zu entziehen, deaktivieren Sie das zugehörige Kontrollkästchen.
   - Um alle Berechtigungen auf eine Tabelle zu entziehen, verwenden Sie das Kontextmenü **Löschen**.

6. (Optional) Um weitere Bedingungen für Tabellenberechtigungen festzulegen, wechseln Sie im unteren Bereich des Berechtigungseditors auf die Ansicht **Berechtigung der Berechtigungsgruppe auf Tabelle** und wählen Sie den Tabreiter **Berechtigungsfilter**.

   HINWEIS: Berechtigungsfilter können Sie nur auf die Tabellen definieren, die Anwendungsdaten abbilden.

   - Erfassen Sie die Bedingungen als gültige Where-Klausel für Datenbankabfragen. Folgende Berechtigungsfilter können Sie erfassen.
     - **Bedingung für Sichtbarkeit**: Einschränkende Bedingung für das Anzeigen der Datensätze.
     - **Bedingung für Bearbeitbarkeit**: Einschränkende Bedingung für das Bearbeiten der Datensätze.
     - **Bedingung für Einfügen**: Einschränkende Bedingung für das Einfügen der Datensätze.
     - **Bedingung für Löschen**: Einschränkende Bedingung für das Löschen der Datensätze.

   Beispiel: 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.

7. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Spaltenberechtigungen bearbeiten auf Seite 66
- Tabellenberechtigungen und Spaltenberechtigungen kopieren auf Seite 67

Spaltenberechtigungen bearbeiten

WICHTIG:

- Wenn Sie Berechtigungen auf Spalten vergeben, müssen ebenfalls Sie die Berechtigungen 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 die Berechtigung **Einfügbar**.
- Wenn Sie die Berechtigungen **Einfügbar** oder **Bearbeitbar** vergeben, wird auch die Berechtigung **Sichtbar** vergeben.
- Über die Spaltendefinition können Sie Skripte zum bedingten Anzeigen oder Bearbeiten einer Spalte verwenden. So kann beispielsweise gesteuert werden, dass eine Spalte auf einem Stammdatenformular im Manager nur angezeigt wird oder bearbeitbar ist, wenn eine andere Spalte einen bestimmten Wert besitzt. Die Skripte verändern nicht die Berechtigungen eines Benutzers, sondern lediglich das Verhalten beim Laden eines Objektes in den One Identity Manager-Werkzeugen. Ausführliche Informationen zum Bearbeiten der Spaltendefinitionen finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

Um für eine Berechtigungsgruppe die Berechtigungen auf eine Spalte zu bearbeiten

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

   TIPP: Mit **Umschalt + Auswahl** oder **Strg +Auswahl** können Sie mehrere Spalten auswählen.
5. Bearbeiten Sie im Bereich **Berechtigungen** die Berechtigungen für die Berechtigungsgruppe.
   - Um neue Berechtigungen einzufügen, wählen Sie das Kontextmenü **Neu** und aktivieren Sie die zugehörigen Kontrollkästchen. Folgende Berechtigungen können Sie vergeben.

- **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.

- Um eine Berechtigung zu entziehen, deaktivieren Sie das zugehörige Kontrollkästchen.
- Um alle Berechtigungen auf eine Spalte zu entziehen, verwenden Sie das Kontextmenü **Löschen**.

6. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Tabellenberechtigungen bearbeiten auf Seite 64
- Tabellenberechtigungen und Spaltenberechtigungen kopieren auf Seite 67

Tabellenberechtigungen und Spaltenberechtigungen kopieren

Um die Berechtigungen einer Berechtigungsgruppe schnell von einer Tabelle auf andere Tabellen zu übernehmen, können Sie die Tabellenberechtigungen und Spaltenberechtigungen kopieren. Dafür werden im Berechtigungseditor zwei Methoden angeboten:

- **Kopieren** und **Einfügen**: Mit der Methode werden die Berechtigungen der Quelltabelle (Quellspalte) einer Berechtigungsgruppe kopiert. Es werden die Berechtigungen der Berechtigungsgruppe kopiert, die Sie in der Symbolleiste des Berechtigungseditors in der Auswahlliste **Berechtigungsgruppe** gewählt haben.

  Es werden alle kopierten Berechtigungen für die Zieltabelle (Zielspalte) eingefügt. Bereits vorhandene Berechtigungen für die Zieltabelle (Zielspalte) bleiben bestehen.
- **Alle Berechtigungen kopieren** und **Alle Berechtigungen einfügen**: Mit der Methode werden die Berechtigungen der Quelltabelle (Quellspalte) kopiert. Die Vorauswahl der Berechtigungsgruppe im Berechtigungseditor spielt keine Rolle. Es werden die Berechtigungen aller Berechtigungsgruppen der Quelltabelle (Quellspalte) übernommen.

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

Um die Berechtigungen einer Berechtigungsgruppe zu kopieren

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Berechtigungseditor über die Aufgabe **Berechtigungen bearbeiten**.
3. Wählen Sie in der Symbolleiste des Berechtigungseditors in der Auswahlliste **Berechtigungsgruppe** die Berechtigungsgruppe, für die Sie die Berechtigungen vergeben möchten.
4. Um die Tabellenberechtigungen zu übernehmen.
    a. Wählen Sie im oberen Bereich der Berechtigungseditors die Tabelle, von der Sie die Berechtigungen übernehmen möchten.
    b. Kopieren Sie die Berechtigungen über das Kontextmenü **Kopieren** in den Zwischenspeicher.
    c. Wählen Sie im oberen Bereich der Berechtigungseditors die Tabelle, für die Sie die Berechtigungen übernehmen möchten.
    d. Fügen Sie die Berechtigungen über das Kontextmenü **Einfügen** ein.
    e. Wiederholen bei Bedarf Sie Schritt c) und d) für weitere Tabellen.
5. Um die Spaltenberechtigungen zu übernehmen
    a. Wählen Sie im oberen Bereich der Berechtigungseditors die Tabelle und wählen Sie die Spalte, von der Sie die Berechtigungen übernehmen möchten.
    b. Kopieren Sie die Berechtigungen über das Kontextmenü **Kopieren**.
    c. Wählen Sie im oberen Bereich der Berechtigungseditors die Tabelle und wählen Sie die Spalte, für die Sie die Berechtigungen übernehmen möchten.
    d. Fügen Sie die Berechtigungen über das Kontextmenü **Einfügen** ein.
    e. Wiederholen bei Bedarf Sie Schritt c) und d) für weitere Spalten.
6. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Tabellenberechtigungen bearbeiten auf Seite 64
- Spaltenberechtigungen bearbeiten auf Seite 66

Berechtigungen für Systembenutzer simulieren

Über die Simulation der Berechtigungen im Berechtigungseditor sehen Sie für einen Systembenutzer, welche Berechtigungen er aufgrund seiner Berechtigungsgruppen besitzt. Sie können festlegen, welche Berechtigungsgruppen eines Systembenutzers in die Simulation aufzunehmen sind. Als Ergebnis wird angezeigt, welche der ausgewählten Berechtigungsgruppen, welche Tabellenberechtigungen und Spaltenberechtigungen

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 Berechtigungen einer Berechtigungsgruppe bearbeiten und die Simulationsdaten aktualisieren.

Um eine Simulation auszuführen

1. Wählen Sie im Designer die Kategorie **Berechtigungen**.
2. Starten Sie den Berechtigungseditor über die Aufgabe **Berechtigungen 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 Berechtigungsgruppen, die dem Systembenutzer direkt zugewiesen sind.
    - **alle Gruppen**: Über diese Schaltfläche wählen Sie alle Berechtigungsgruppen, die dem Systembenutzer direkt zugewiesen sind sowie alle Berechtigungsgruppen, die der Systembenutzer indirekt erbt.
    - **Gruppen**: Wählen Sie einzelne Berechtigungsgruppen direkt aus. Über **Umschalt + Auswahl** können Sie mehrere Berechtigungsgruppen auswählen.
6. Auf der Seite **Simulationskonfiguration** legen Sie fest, für welche Tabellen die Berechtigungen simuliert werden.
    - Im Bereich **Ausgewählte Tabellen** sind alle Tabellen des One Identity Manager Schemas ausgewählt. Schränken Sie die Auswahl bei Bedarf auf einzelne Tabellen ein. Klicken Sie **Keine** um die Auswahl aufzuheben. Wählen Sie mit **Umschalt + Auswahl** einzelne Tabellen aus.
    - Über die Auswahlliste **Kontexttabelle** können Sie eine Tabelle festlegen, aus deren Sicht sich implizite Berechtigungen auf die Anzeigewerte der Fremdschlüsselspalten ergeben.

      Beispiel:

      Für die Tabelle `Person` wurden Sichtbarkeitsberechtigungen auf die Spalte `UID_Org` vergeben. Damit werden implizit die Sichtbarkeitsberechtigungen 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 Berechtigungseditors im Bereich **Simulation** die effektiven Tabellenberechtigungen und Spaltenberechtigungen des Systembenutzers angezeigt.
9. Um zu ermitteln, aus welchen Berechtigungsgruppen des Systembenutzers, welche Tabellenberechtigung oder welche Spaltenberechtigung resultiert, wählen Sie die Tabelle oder Spalte im oberen Bereich des Berechtigungseditors.

   Im unteren Bereich des Berechtigungseditors werden in der Ansicht **Simulation der Berechtigungen** die Berechtigungen und Berechtigungsgruppen angezeigt.
10. Um den Simulationsmodus zu beenden, wählen Sie das Menü **Simulation > Simulation beenden**.

    Die Simulationsdaten werden gelöscht und die Ansicht **Simulation der Berechtigungen** wird geschlossen.

Berechtigungen für Objekte anzeigen

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

HINWEIS: Der Manager muss zur Anzeige der Eigenschaften eines Objektes im Expertenmodus laufen.

Um Berechtigungen eines Objektes anzuzeigen

1. Wählen Sie das Objekt und öffnen Sie das Kontextmenü **Eigenschaften**.
2. Wählen Sie den Tabreiter **Berechtigungen**.

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

   TIPP: Doppelklicken Sie auf den Tabelleneintrag, den Objekteintrag oder einen Spalteneintrag, um die Berechtigungsgruppen 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 des Programms auf das Symbol .

Tabelle 27: Erweiterte Informationen zum angemeldeten Benutzer

Eigenschaft	Bedeutung
Systembenutzer	Bezeichnung des verwendeten Systembenutzers.
Authentifiziert durch	Bezeichnung des Authentifizierungsmoduls, das zur Anmeldung verwendet wird.
UID der Person (UserUID)	Eindeutige Kennung der Person des angemeldeten Benutzers, falls ein personenbezogenes Authentifizierungsmodul zur Anmeldung benutzt wird.
SQL Berechtigungsebene	Berechtigungsebene der verwendeten Datenbankserver-Anmeldung.
Nur Leseberechtigungen	Der verwendete Systembenutzer besitzt nur Berechtigungen zum Lesen. Datenänderungen sind nicht möglich.
Dynamischer Benutzer	Der angemeldete Benutzer verwendet einen dynamischen Systembenutzer. Dynamische Systembenutzer werden eingesetzt, wenn zur Anmeldung ein rollenbasiertes Authentifizierungsmodul benutzt wird.
Administrativer Benutzer	Der angemeldete Benutzer verwendet einen administrativen Systembenutzer.
Bemerkungen	Nähere Beschreibung zum verwendeten Systembenutzer.
Berechtigungsgruppen	Berechtigungsgruppen, die dem Systembenutzer zugewiesen sind. Abhängig von den Berechtigungsgruppen erhält der Benutzer die Benutzeroberfläche und die Berechtigungen auf die Objekte.

Eigenschaft	Bedeutung
Programmfunktionen	Programmfunktionen, die dem Systembenutzer zugewiesen sind. Abhängig von den Programmfunktionen werden Menüeinträge und Funktionen zur Verfügung gestellt.

Rollenbasierte Berechtigungsgruppen an Anwendungen zuweisen

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

Um eine rollenbasierte Berechtigungsgruppe an eine Anwendung zuzuweisen

1. Wählen Sie im Designer die Kategorie **Berechtigungen > Berechtigungsgruppen > Rollenbasierte Berechtigungsgruppen**.
2. Wählen Sie den Menüeintrag **Ansicht > Tabellenrelationen wählen** und aktivieren Sie die Tabelle `DialogGroupInProductLimited`.
3. Wählen Sie im Listeneditor die Berechtigungsgruppe.
4. Weisen Sie in der Bearbeitungsansicht **Anwendung** die Anwendung zu.
5. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

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

Steuern von Berechtigungen über Programmfunktionen

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

- Berechtigungen der angemeldeten Benutzer anzeigen auf Seite 71
- Programmfunktionen an Berechtigungsgruppen zuweisen auf Seite 74
- Berechtigungen zum Ausführen von Skripten auf Seite 74
- Berechtigungen zum Ausführen von Methoden auf Seite 76
- Berechtigungen zum Auslösen von Prozessen auf Seite 77
- Berechtigungen zum Ausführen von Aktionen im Launchpad auf Seite 78
- Programmfunktionen zum Starten der One Identity Manager-Werkzeuge auf Seite 160

Programmfunktionen des angemeldeten Benutzers anzeigen

Um die verfügbaren Programmfunktionen für den angemeldeten Benutzer zu ermitteln

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

  Auf dem Tabreiter **Programmfunktionen** werden die verfügbaren Programmfunktionen angezeigt.

Programmfunktionen an Berechtigungsgruppen zuweisen

Um eine Programmfunktion an Berechtigungsgruppen 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 **Berechtigungsgruppe** die Berechtigungsgruppen zu.
5. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Systembenutzer in Berechtigungsgruppen aufnehmen auf Seite 59

Berechtigungen zum Ausführen von Skripten

Die grundlegende Berechtigung zum Ausführen von Skripten erhält der angemeldete Benutzer über die Programmfunktion **Common_StartScripts**.

Wird ein Skript zusätzlich mit einer Programmfunktion versehen (Tabelle `QBMScriptHasFeature`), so kann ein Benutzer dieses Skript nur noch ausführen, wenn er auch die nötige Programmfunktion über seine Berechtigungsgruppen besitzt. Besitzt der

Benutzer die Programmfunktion nicht, so wird beim Ausführungsversuch eine Fehlermeldung geworfen.

Um die Ausführung eines Skriptes über eine Programmfunktion zu steuern

1. Erstellen Sie eine neue Programmfunktion.
    a. Wählen Sie im Designer die Kategorie **Berechtigungen > Programmfunktionen**.
    b. Wählen Sie den Menüeintrag **Objekt > Neu**.
    c. Erfassen Sie die folgenden Informationen:
        - **Programmfunktion**: Bezeichnung der Programmfunktion.
        - **Beschreibung**: Kurze Beschreibung der Programmfunktion.
        - **Funktionsgruppe**: Merkmal zu Gruppierung von Programmfunktionen.
2. Verbinden Sie die Programmfunktion mit den Skripten, die die Benutzer auslösen dürfen.
    a. Wählen Sie im Designer die Kategorie **Berechtigungen > Programmfunktionen**.
    b. Wählen Sie den Menüeintrag **Ansicht > Tabellenrelationen wählen** und aktivieren Sie die Tabelle `QBMScriptHasFeature`.
    c. Wählen Sie im Listeneditor die neu erstellte Programmfunktion.
    d. Weisen Sie in der Bearbeitungsansicht **Skripte** die Skripte zu.
3. Weisen Sie die Programmfunktion an die kundenspezifische Berechtigungsgruppe 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 **Common_StartScripts**.
    e. Weisen Sie in der Bearbeitungsansicht **Berechtigungsgruppe** die Berechtigungsgruppe zu.
4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Bearbeitung von Berechtigungsgruppen auf Seite 49

Berechtigungen zum Ausführen von Methoden

Wird eine Methodendefinition mit einer Programmfunktion (Tabelle `QBMMethodHasFeature`) versehen, so kann ein Benutzer diese Methode nur noch ausführen, wenn er auch die nötige Programmfunktion über seine Berechtigungsgruppen besitzt. Besitzt der Benutzer die Programmfunktion nicht, so wird beim Ausführungsversuch eine Fehlermeldung geworfen.

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

1. Erstellen Sie eine neue Programmfunktion.
    a. Wählen Sie im Designer die Kategorie **Berechtigungen > Programmfunktionen**.
    b. Wählen Sie den Menüeintrag **Objekt > Neu**.
    c. Erfassen Sie die folgenden Informationen:
        - **Programmfunktion**: Bezeichnung der Programmfunktion.
        - **Beschreibung**: Kurze Beschreibung der Programmfunktion.
        - **Funktionsgruppe**: Merkmal zu Gruppierung von Programmfunktionen.
2. Verbinden Sie die Programmfunktion mit den Methodendefinitionen, die die Benutzer auslösen sollen.
    a. Wählen Sie im Designer die Kategorie **Berechtigungen > Programmfunktionen**.
    b. Wählen Sie den Menüeintrag **Ansicht > Tabellenrelationen wählen** und aktivieren Sie die Tabelle `QBMMethodHasFeature`.
    c. Wählen Sie im Listeneditor die neu erstellte Programmfunktion.
    d. Weisen Sie in der Bearbeitungsansicht **Methoden** die Methodendefinitionen zu.
3. Weisen Sie die Programmfunktion an die kundenspezifische Berechtigungsgruppe 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 **Berechtigungsgruppe** die Berechtigungsgruppe zu.
4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Bearbeitung von Berechtigungsgruppen auf Seite 49

Berechtigungen zum Auslösen von Prozessen

Die grundlegende Berechtigung zum Auslösen von Prozessen erhält der angemeldete Benutzer über die Programmfunktion **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 Bearbeitungsberechtigungen besitzen. Dies kann dazu führen, dass Benutzer an Tabellen, für die nur Sichtbarkeitsberechtigungen 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. Das Objektereignis wird mit einer Programmfunktion (Tabelle `QBMEventHasFeature`) verbunden. Benutzer mit dieser Programmfunktion können, unabhängig von ihren Berechtigungen, das Objektereignis und damit auch den Prozess auslösen.

TIPP: Die Programmmfunktion **Common_TriggerSpecificEvents** ermöglicht das Auslösen bestimmter Ereignisse vom Frontend aus. Diese Programmmfunktion können Sie an kundenspezifische Objektereignissen zuweisen, die jeder Benutzer auslösen können soll. Die Programmfunktion ist der Berechtigungsgruppe **QBM_BaseRight** zugewiesen.

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 **Objektereignis** die Objektereignisse zu.

3. Weisen Sie die benötigten Programmfunktionen an die kundenspezifische Berechtigungsgruppe 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 **Common_TriggerEvents**.

d. Weisen Sie in der Bearbeitungsansicht **Berechtigungsgruppe** die Berechtigungsgruppe zu.

4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Bearbeitung von Berechtigungsgruppen auf Seite 49

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 Aktion** die Aktionen zu.

5. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

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 Berechtigungsgruppen die Benutzeroberfläche und die Berechtigungen auf Ressourcen der Datenbank.

- Für die Anmeldung an den One Identity Manager-Werkzeugen mit einem Authentifizierungsmodul, das einen definierten Systembenutzer erwartet, werden die Berechtigungen aus den Berechtigungsgruppen 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 Berechtigungsgruppen zu One Identity Manager Anwendungsrollen wird bestimmt, welche Berechtigungsgruppen für die Person gültig sind. Aus diesen Berechtigungsgruppen wird ein dynamischer Systembenutzer berechnet, der für die Anmeldung der Person benutzt wird.

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

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

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

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

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

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

Verwandte Themen

- Authentifizierungsmodule aktivieren auf Seite 117
- Authentifizierungsmodule zu Anwendungen zuweisen auf Seite 118
- Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren auf Seite 118

Systembenutzer

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

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 Berechtigungen 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 Berechtigungen 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 Konfigurationsparameter 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 Berechtigungen 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 28: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
QER | Person | GenericAuthenticator	Gibt an, ob die Authentifizierung über Single Sign-on unterstützt wird.
QER | Person | GenericAuthenticator | SearchTable	Tabelle im One Identity Manager Schema in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens `UID_Person` (oder `CCC_UID_Person`) enthalten, der auf die Tabelle `Person` zeigt. Beispiel: `ADSAccount`
QER | Person | GenericAuthenticator | SearchColumn	Spalte aus der One Identity Manager Tabelle (**SearchTable**), die zur Suche des Benutzernamens des angemeldeten Benutzers verwendet wird. Beispiel: `CN`
QER | Person | GenericAuthenticator | EnabledBy	Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (**SearchTable**), die das Benutzerkonto für die Anmeldung aktiviert.
QER | Person | GenericAuthenticator | DisabledBy	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 Konfigurationsparameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. Die Benutzeroberfläche und die Berechtigungen 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 Konfigurationsparameter 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 Berechtigungen 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	ja

Portal möglich	
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 Konfigurationsparameter 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 Berechtigungen 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 125

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 Konfigurationsparameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. Die Benutzeroberfläche und die Berechtigungen 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 Konfigurationsparameter 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 Berechtigungen werden über diesen Systembenutzer geladen. Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Benutzerkonto (manuelle Eingabe/rollenbasiert)

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Identity Management Basismodul 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. • In den Personenstammdaten sind die zulässigen Anmeldungen eingetragen. Die Anmeldungen werden in der Form **Domäne\Benutzer** erwartet.

	• Die Person ist mindestens einer Anwendungsrolle zugewiesen. • Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter **TargetSystem | ADS | AuthenticationDomains** eingetragen. HINWEIS: Der Konfigurationsparameter steht zur Verfügung, wenn das Active Directory Modul vorhanden ist.
Aktiviert im Standard	ja
Single Sign-on	nein
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. Dabei wird die Liste der zulässigen Active Directory Domänen berücksichtigt. 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 Konfigurationsparameter 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 Berechtigungen werden über diesen Systembenutzer geladen. Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Kontobasierter Systembenutzer

HINWEIS: Dieses Authentifizierungsmodul steht zur Verfügung, wenn das Konfigurationsmodul 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. • 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 Berechtigungen 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 Konfigurationsparameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. Die Benutzeroberfläche und die Berechtigungen 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 Konfigurationsparameter 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 Berechtigungen 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 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	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 Konfigurationsparameter 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 Berechtigungen 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 Konfigurationsparameter 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 Berechtigungen 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 Konfigurationsparameter 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 Berechtigungen 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 125

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 das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter **TargetSystem | LDAP | Authentication | RootDN** beziehungsweise im Konfigurationsparameter **TargetSystem | LDAP | AuthenticationV2 | RootDN** eingetragen. Erfolgt die Anmeldung über den definierten Namen, wird das LDAP Benutzerkonto ermittelt, das diesen definierten Namen verwendet. Der One Identity Manager ermittelt die Person, die dem LDAP Benutzerkonto zugeordnet ist. Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird. • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Konfigurationsparameter 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 Berechtigungen 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 29: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
TargetSystem | LDAP | Authentication	Erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem | LDAP | Authentication | Authentication	Authentifizierungsmechanismus. 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: **ServerBind**
TargetSystem | LDAP | Authentication | Port	Kommunikationsport auf dem Server. Standard: **389**

TargetSystem | LDAP | Authentication | RootDN	Pipe (|) getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.
	Syntax:
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Beispiel:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | Authentication | Server	Name des LDAP Servers.
TargetSystem | LDAP | AuthenticationV2	Erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem | LDAP | AuthenticationV2 | AcceptSelfSigned	Gibt an, ob selbstsignierte Zertifikate akzeptiert werden.
TargetSystem | LDAP | AuthenticationV2 | Authentication	Authentifizierungsmethode zur Anmeldung am LDAP System. Zulässig sind: • **Basic**: Die Standardauthentifizierung wird verwendet. • **Negotiate**: Die Negotiate-Authentifizierung von Microsoft wird verwendet. • **Kerberos**: Die Kerberos-Authentifizierung wird verwendet. • **NTLM**: Die Windows NT-Abfrage/Rückmeldung-Authentifizierung wird verwendet.

Konfigurationsparameter	Bedeutung
	Standard: **Basic** Weitere Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
TargetSystem | LDAP | AuthenticationV2 | ClientTimeout	Client-Timeout in Sekunden.
TargetSystem | LDAP | AuthenticationV2 | Port	Kommunikationsport auf dem Server. Standard: **389**
TargetSystem | LDAP | AuthenticationV2 | ProtocolVersion	Version des LDAP Protokolls. Zulässig sind die Werte **2** und **3**. Standard: **3**

TargetSystem | LDAP | AuthenticationV2 | RootDN	Pipe (|) getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.
	Syntax:
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Beispiel:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | AuthenticationV2 | Security	Sicherheit der Verbindung. Zulässige Werte sind **None**, **SSL** und **STARTTLS**.
TargetSystem | LDAP | AuthenticationV2 | Server	Name des LDAP Servers.
TargetSystem | LDAP | AuthenticationV2 | UseSealing	Gibt an, ob die Nachrichtenvertraulichkeit aktiviert ist.
TargetSystem | LDAP | AuthenticationV2 | UseSigning	Gibt an, ob Nachrichtenintegrität aktiviert ist.
TargetSystem | LDAP | AuthenticationV2 | VerifyServerCertificate	Gibt an, ob bei Verschlüsselung mit SSL das Serverzertifikat geprüft werden soll.

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 das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Die zulässigen Domänen für die Anmeldung sind im Konfigurationsparameter **TargetSystem | LDAP | Authentication | RootDN** beziehungsweise im Konfigurationsparameter **TargetSystem | LDAP | AuthenticationV2 | RootDN** eingetragen. Erfolgt die Anmeldung über den definierten Namen, wird das LDAP Benutzerkonto ermittelt, das diesen definierten Namen verwendet. Der One Identity Manager ermittelt die Person, die dem LDAP Benutzerkonto zugeordnet ist. Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter **QER | Person | MasterIdentity | UseMasterForAuthentication** gesteuert, welche Person zur Authentifizierung verwendet wird. • Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt. • Ist der Konfigurationsparameter 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 Berechtigungen 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 30: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
TargetSystem | LDAP | Authentication	Erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem | LDAP | Authentication | Authentication	Authentifizierungsmechanismus. 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: **ServerBind**
TargetSystem | LDAP | Authentication | Port	Kommunikationsport auf dem Server. Standard: **389**

TargetSystem | LDAP | Authentication | RootDN	Pipe (|) getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.
	Syntax:
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Beispiel:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | Authentication | Server	Name des LDAP Servers.
TargetSystem | LDAP | AuthenticationV2	Erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem | LDAP | AuthenticationV2 | AcceptSelfSigned	Gibt an, ob selbstsignierte Zertifikate akzeptiert werden.
TargetSystem | LDAP | AuthenticationV2 | Authentication	Authentifizierungsmethode zur Anmeldung am LDAP System. Zulässig sind: • **Basic**: Die Standardauthentifizierung wird

Konfigurationsparameter	Bedeutung
	verwendet. • **Negotiate**: Die Negotiate-Authentifizierung von Microsoft wird verwendet. • **Kerberos**: Die Kerberos-Authentifizierung wird verwendet. • **NTLM**: Die Windows NT-Abfrage/Rückmeldung-Authentifizierung wird verwendet. Standard: **Basic** Weitere Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
TargetSystem | LDAP | AuthenticationV2 | ClientTimeout	Client-Timeout in Sekunden.
TargetSystem | LDAP | AuthenticationV2 | Port	Kommunikationsport auf dem Server. Standard: **389**
TargetSystem | LDAP | AuthenticationV2 | ProtocolVersion	Version des LDAP Protokolls. Zulässig sind die Werte **2** und **3**. Standard: **3**

TargetSystem | LDAP | AuthenticationV2 | RootDN	Pipe (|) getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.
	Syntax:
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Beispiel:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | AuthenticationV2 | Security	Sicherheit der Verbindung. Zulässige Werte sind **None**, **SSL** und **STARTTLS**.
TargetSystem | LDAP | AuthenticationV2 | Server	Name des LDAP Servers.
TargetSystem | LDAP | AuthenticationV2 | UseSealing	Gibt an, ob die Nachrichtenvertraulichkeit aktiviert ist.
TargetSystem | LDAP | AuthenticationV2 | UseSigning	Gibt an, ob Nachrichtenintegrität aktiviert ist.
TargetSystem | LDAP | AuthenticationV2 | VerifyServerCertificate	Gibt an, ob bei Verschlüsselung mit SSL das Serverzertifikat geprüft werden soll.

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 125

HTTP Header

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

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 Konfigurationsparameter deaktiviert, wird die

Subidentität der Person für die Authentifizierung genutzt.

Die Benutzeroberfläche und die Berechtigungen 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)

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

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 Konfigurationsparameter 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 Berechtigungen 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 Konfigurationsparameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. Die Benutzeroberfläche und Berechtigungen 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.

HINWEIS: Wenn für den Claim-Wert keine passende Person gefunden wird, sucht das Authentifizierungsmodul den Claim-Wert in den zulässigen Anmeldungen der Systembenutzer (`DialogUser.AuthentifierLogons`). Gibt es dort einen Eintrag, wird dieser Systembenutzer angemeldet. Für Zuordnung von Datenänderungen werden die Werte aus den entsprechenden Claims genutzt. Wenn eine passende Person gefunden wird, wird der Fallback nicht mehr angewendet.

Verwandte Themen

- OAuth 2.0/OpenID Connect Authentifizierung auf Seite 132
- Ablauf der OAuth 2.0/OpenID Connect Authentifizierung auf Seite 133

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 Konfigurationsparameter 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 Berechtigungen 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.

HINWEIS: Wenn für den Claim-Wert keine passende Person gefunden wird, sucht das Authentifizierungsmodul den Claim-Wert in den zulässigen Anmeldungen der Systembenutzer (`DialogUser.AuthentifierLogons`). Gibt es dort einen Eintrag, wird dieser Systembenutzer angemeldet. Für Zuordnung von Datenänderungen werden die Werte

aus den entsprechenden Claims genutzt. Wenn eine passende Person gefunden wird, wird der Fallback nicht mehr angewendet.

Verwandte Themen

- OAuth 2.0/OpenID Connect Authentifizierung auf Seite 132
- Ablauf der OAuth 2.0/OpenID Connect Authentifizierung auf Seite 133

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

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

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

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

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

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

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. - ODER - Zielsystembenutzerkonto und Zugangscode. - ODER - Zielsystembenutzerkonto und Antworten auf die Kennwortabfragen.
Voraussetzungen	• Die Person ist in der One Identity Manager-Datenbank vorhanden. • Bei Verwendung des zentralen Benutzerkontos: In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen. • Bei Verwendung des Zielsystembenutzerkontos: Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist

	die Person eingetragen. • Die Person ist nicht deaktiviert oder hat den Zertifizierungsstatus **Neu**. • Die Person hat einen Zugangscode oder die Fragen und Antworten zur Kennwortabfrage sind hinterlegt.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	Das Anwendungstoken für das 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*.

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

Tabelle 31: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
QER | Person | PasswordResetAuthenticator | SearchTable	Tabelle im One Identity Manager Schema in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens `UID_Person` (oder `CCC_UID_Person`) enthalten, der auf die Tabelle `Person` zeigt. Beispiel: `ADSAccount`
QER | Person | PasswordResetAuthenticator | SearchColumn	Pipe (|) getrennte Liste von Spalten aus der One Identity Manager Tabelle (**SearchTable**), die zur Suche des Benutzernamens des angemeldeten Benutzers verwendet werden. Beispiel: `CN|SamAccountName` HINWEIS: Als Suchtabelle kann die Tabelle `QBMSplittedLookup` genutzt werden. Als Suchspalte

Konfigurationsparameter	Bedeutung
	kann `SplittedElement` verwendet werden.
QER | Person | PasswordResetAuthenticator | EnabledBy	Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (**SearchTable**), die das Benutzerkonto für die Anmeldung aktivieren.
QER | Person | PasswordResetAuthenticator | DisabledBy	Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (**SearchTable**), die das Benutzerkonto für die Anmeldung deaktivieren. Beispiel: `AccountDisabled`

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. - ODER - Zielsystembenutzerkonto und Zugangscode. - ODER - Zielsystembenutzerkonto und Antworten auf die Kennwortabfragen.
Voraussetzungen	• Die Person ist in der One Identity Manager-Datenbank vorhanden. • Bei Verwendung des zentralen Benutzerkontos: In den Personenstammdaten ist das zentrale Benutzerkonto eingetragen. • Bei Verwendung des Zielsystembenutzerkontos: Das Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen. • Die Person ist nicht deaktiviert oder hat den

	Zertifizierungsstatus **Neu**. • Die Person hat einen Zugangscode oder die Fragen und Antworten zur Kennwortabfrage sind hinterlegt. • Die Person ist mindestens einer Anwendungsrolle zugewiesen.
Aktiviert im Standard	ja
Single Sign-on	nein
Anmeldung am Frontend möglich	nein
Anmeldung am Web Portal möglich	nein
Bemerkungen	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 Berechtigungen werden über diesen Systembenutzer geladen.

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

Tabelle 32: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
QER | Person | PasswordResetAuthenticator | SearchTable	Tabelle im One Identity Manager Schema in der die Benutzerinformationen hinterlegt werden. Die Tabelle muss einen Fremdschlüssel namens `UID_Person` (oder `CCC_UID_Person`) enthalten, der auf die Tabelle `Person` zeigt. Beispiel: `ADSAccount`
QER | Person | PasswordResetAuthenticator | SearchColumn	Pipe (|) getrennte Liste von Spalten aus der One Identity Manager Tabelle (**SearchTable**), die zur Suche des Benutzernamens des angemeldeten Benutzers

Konfigurationsparameter	Bedeutung
	verwendet werden. Beispiel: `CN|SamAccountName` HINWEIS: Als Suchtabelle kann die Tabelle `QBMSplittedLookup` genutzt werden. Als Suchspalte kann `SplittedElement` verwendet werden.
QER | Person | PasswordResetAuthenticator | EnabledBy	Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (**SearchTable**), die das Benutzerkonto für die Anmeldung aktivieren.
QER | Person | PasswordResetAuthenticator | DisabledBy	Pipe (|) getrennte Liste von Boolean-Spalten aus der One Identity Manager Tabelle (**SearchTable**), die das Benutzerkonto für die Anmeldung deaktivieren. Beispiel: `AccountDisabled`

Dezentrale Identität

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

Das Authentifizierungsmodul kann zur Anmeldung über eine dezentrale Identität genutzt werden.

Anmeldeinformationen	E-Mail-Adresse und dezentrale Identität 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 die dezentrale Identität eingetragen. • In den Personenstammdaten ist die Standard-E-Mail-Adresse oder die Kontakt-E-Mail-Adresse eingetragen. • In den Personenstammdaten ist der Systembenutzer eingetragen.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web	ja

Portal möglich	
Bemerkungen	Um die Person zu ermitteln, wird die E-Mail-Adresse, die bei der Anmeldung angegeben wird, gegen die Standard-E-Mail-Adresse und die Kontakt-E-Mail-Adresse geprüft. 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 Konfigurationsparameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt. Die Benutzeroberfläche und die Berechtigungen werden über den Systembenutzer geladen, der der angemeldeten Person direkt zugeordnet ist. Datenänderungen werden der angemeldeten Person zugeordnet.

Dezentrale Identität (rollenbasiert)

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

Das Authentifizierungsmodul kann zur Anmeldung über eine dezentrale Identität genutzt werden.

Anmeldeinformationen	E-Mail-Adresse und dezentrale Identität der Person.
Voraussetzungen	• Die Person ist in der One Identity Manager-Datenbank vorhanden. • In den Personenstammdaten ist die dezentrale Identität eingetragen. • In den Personenstammdaten ist die Standard-E-Mail-Adresse oder die Kontakt-E-Mail-Adresse eingetragen. • Die Person ist mindestens einer Anwendungsrolle zugewiesen.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja

Anmeldung am Web Portal möglich	ja
Bemerkungen	Um die Person zu ermitteln, wird die E-Mail-Adresse, die bei der Anmeldung angegeben wird, gegen die Standard-E-Mail-Adresse und die Kontakt-E-Mail-Adresse geprüft. 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 Konfigurationsparameter 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 Berechtigungen werden über diesen Systembenutzer geladen. Datenänderungen werden der angemeldeten Person zugeordnet.

Bearbeiten der Authentifizierungsmodule

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

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

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

Detaillierte Informationen zum Thema

- Authentifizierungsmodule aktivieren auf Seite 117
- Authentifizierungsmodule zu Anwendungen zuweisen auf Seite 118
- Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren auf Seite 118

- Eigenschaften von Authentifizierungsmodulen auf Seite 119
- Initiale Daten für Authentifizierungsmodule auf Seite 120
- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 125
- One Identity Manager Authentifizierungsmodule auf Seite 80
- Steuern von Berechtigungen über Programmfunktionen auf Seite 73
- Programmfunktionen zum Starten der One Identity Manager-Werkzeuge auf Seite 160

Authentifizierungsmodule aktivieren

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

Um ein Authentifizierungsmodul für die Anmeldung zu nutzen, müssen Sie das Authentifizierungsmodul aktivieren.

Um ein Authentifizierungsmodul für die Anmeldung zu nutzen, müssen Sie das Authentifizierungsmodul aktivieren. Führen Sie die folgenden Schritte aus, um ein Authentifizierungsmodul zu 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. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren auf Seite 118
- Authentifizierungsmodule zu Anwendungen zuweisen auf Seite 118

Authentifizierungsmodule zu Anwendungen zuweisen

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

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 eine Anwendung 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. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren auf Seite 118
- Authentifizierungsmodule aktivieren auf Seite 117

Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren

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

Um ein Authentifizierungsmodul zur Anmeldung zu verwenden, muss die Zuweisung des Authentifizierungsmoduls zur Anwendung aktiviert sein.

Um ein Authentifizierungsmodul für eine Anwendung zu aktivieren

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. Wählen Sie in der Bearbeitungsansicht **Anwendung** die zugewiesene Anwendung.
5. Deaktivieren Sie die Option **Deaktiviert**.
6. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Um ein Authentifizierungsmodul für eine Anwendung zu deaktivieren

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. Wählen Sie in der Bearbeitungsansicht **Anwendung** die zugewiesene Anwendung.
5. Aktivieren Sie die Option **Deaktiviert**.
6. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Authentifizierungsmodule zu Anwendungen zuweisen auf Seite 118
- Authentifizierungsmodule aktivieren auf Seite 117

Eigenschaften von Authentifizierungsmodulen

Tabelle 33: Eigenschaften von Authentifizierungsmodulen

Eigenschaft	Bedeutung
Aktiviert	Gibt an, ob das Authentifizierungsmoduls zur Verwendung aktiviert ist.
Anzeigename	Anzeigename zur Anzeige des Authentifizierungsmoduls im Verbindungsdialog der Administrationswerkzeuge.
Authentifizierungsmodul	Interner Name des Authentifizierungsmoduls.
Authentifizierungstyp	Typ des Authentifizierungsmoduls. Zur Auswahl stehen **Dynamisch** und **Rollenbasiert**.
Bearbeitungsstatus	Der Bearbeitungsstatus wird bei der Erstellung von Kunden-

Eigenschaft	Bedeutung
	konfigurationspaketen genutzt.

Initiale Daten	Initiale Daten für die Anmeldung mit diesem Authentifizierungsmodul.
	Syntax:
	`Property1=Value1;Property2=Value2`
	Beispiel:
	`User=<user name>;Password=<password>`

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

Verwandte Themen

- Authentifizierungsmodule aktivieren auf Seite 117
- Authentifizierungsmodule zu Anwendungen zuweisen auf Seite 118
- Authentifizierungsmodule für Anwendungen deaktivieren oder aktivieren auf Seite 118
- Initiale Daten für Authentifizierungsmodule auf Seite 120

Initiale Daten für Authentifizierungsmodule

Die Authentifizierungsdaten werden aus dem Authentifizierungsmodul und seinen Parameter mit den Werten gebildet. Für die Parameter und ihre Werte können Sie initiale Daten vorgeben. Die initialen Daten werden bei jedem Authentifizierungsvorgang als Standard vorbelegt.

Syntax für Authentifizierungsdaten:

`Module=<Authenticiation module>;<Property1>=<Value1>;<Property2>=<Value2>,…`

Beispiel:

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

Um initiale Daten für Authentifizierungsmodule 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=Value1;Property2=Value2
   ```

   Beispiel:

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

Tabelle 34: Authentifizierungsdaten für Authentifizierungsmodule

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

Authentifizierungsmodul	Anzeigename	Parameter und Bedeutung
RoleBasedManualADS	Active Directory Benutzerkonto (manuelle Eingabe/rollenbasiert)	**User**: Benutzername. Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Die zulässigen Active Directory Domänen geben Sie im Konfigurationsparameter **TargetSystem | ADS | AuthenticationDomains** an. **Password**: Kennwort des Benutzers.
Person	Person	**User**: Zentrales Benutzerkonto der Person. **Password**: Kennwort des Benutzers.
DynamicPerson	Person (dynamisch)	**Product**: Anwendung. Der Systembenutzer wird über die Konfigurationsdaten der Anwendung bestimmt. **User**: Benutzername. **Password**: Kennwort des Benutzers.
RoleBasedPerson	Person (rollenbasiert)	**User**: Benutzername. **Password**: Kennwort des Benutzers.
HTTPHeader	HTTP Header	**Header**: Zu nutzender HTTP Header. **KeyColumn**: Kommagetrennte Liste der Schlüsselspalten in der Tabelle `Person`, in denen nach dem Benutzernamen gesucht werden soll. Standard: `CentralAccount, PersonnelNumber`
RoleBasedHTTPHeader	HTTP Header (rollenbasiert)	**Header**: Zu nutzender HTTP Header. **KeyColumn**: Kommagetrennte Liste der Schlüsselspalten in

Authentifizierungsmodul	Anzeigename	Parameter und Bedeutung
		Tabelle `Person`, in denen nach dem Benutzernamen gesucht werden soll. Standard: `CentralAccount`, `PersonnelNumber`
DynamicLdap	LDAP Benutzerkonto (dynamisch)	**User**: Benutzername. Standard: `CN`, `DistinguishedName`, `UserID`, `UIDLDAP` **Password**: Kennwort des Benutzers.
RoleBasedLdap	LDAP Benutzerkonto (rollenbasiert)	**User**: Benutzername. Standard: `CN`, `DistinguishedName`, `UserID`, `UIDLDAP` **Password**: Kennwort des Benutzers.
RoleBasedGeneric	Single Sign-on generisch (rollen-basiert)	**SearchTable**: Tabelle, in welcher nach dem Benut-zernamen des angemeldeten Benutzers gesucht wird. Diese Tabelle muss einen FK mit der Bezeichnung `UID_Person` enthalten, der auf die Tabelle `Person` zeigt. **SearchColumn**: Spalte aus der `SearchTable`, in welcher nach dem Benutzernamen des angemeldeten Benutzers gesucht wird. **DisabledBy**: Durch Pipe (|) getrennte Liste von booleschen Spalten, welche ein Benut-zerkonto für das Anmelden sperren. **EnabledBy**: Durch Pipe (|) getrennte Liste von booleschen Spalten, welche ein Benut-zerkonto für das Anmelden freischalten.

Authentifizierungsmodul	Anzeigename	Parameter und Bedeutung
OAuth	OAuth 2.0/OpenID Connect	Abhängig vom Authentifizierungsverfahren des Sicherheitstokendienstes.
OAuthRoleBased	OAuth 2.0/OpenID Connect (rollenbasiert)	Abhängig vom Authentifizierungsverfahren des Sicherheitstokendienstes.
DialogUserAccountBased	Kontobasierter Systembenutzer	Keine Parameter erforderlich.
QERAccount	Benutzerkonto	Keine Parameter erforderlich.
RoleBasedQERAccount	Benutzerkonto (rollenbasiert)	Keine Parameter erforderlich.
RoleBasedManualQERAccount	Benutzerkonto (manuelle Eingabe/rollenbasiert)	**User**: Benutzername. Anhand einer vordefinierten Liste von zulässigen Active Directory Domänen wird die Identität des Benutzers ermittelt. Die zulässigen Active Directory Domänen geben Sie im Konfigurationsparameter **TargetSystem | ADS | AuthenticationDomains** an. **Password**: Kennwort des Benutzers.
PasswordReset	Kennwortrücksetzung	Keine Parameter erforderlich.
RoleBasedPasswordReset	Kennwortrücksetzung (rollenbasiert)	Keine Parameter erforderlich.
DecentralizedId	Dezentrale Identität	**Email**: Standard-E-Mail-Adresse der Person (`Person.DefaultEmailAddress`) oder Kontakt-E-Mail-Adresse der Person (`Person.ContactEmail`) **Identifier**: Dezentrale Identität der Person (`Person.DecentralizedIdentifier`).
RoleBasedDecentralizedId	Dezentrale Identität (rollenbasiert)	**Email**: Standard-E-Mail-Adresse der Person (`Person.DefaultEmailAddress`) oder Kontakt-E-Mail-Adresse der Person (`Person.ContactEmail`)

Authentifizierungsmodul	Anzeigename	Parameter und Bedeutung
		Identifier: Dezentrale Identität der Person (`Person.DecentralizedIdentifier`).
Token		Internes Authentifizierungsmodul im Anwendungsserver für die Authentifizierung über OAuth 2.0/OpenID Connect Zugriffstoken. Weitere Informationen finden Sie unter OAuth 2.0/OpenID Connect Authentifizierung an der REST API des Anwendungsservers auf Seite 144. **URL**: URL des Anwendungsservers **ClientId**: ID der Anwendung beim Identitätsanbieter. **ClientSecret**: Secret-Wert für die Authentifizierung am Tokenendpunkt. **TokenEndpoint**: URL des Tokenendpunktes des Autorisierungsservers für die Rückgabe des Zugriffstokens an den Client für die Anmeldung

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 125
- One Identity Manager Authentifizierungsmodule auf Seite 80

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.

TIPP: Aktivieren Sie für Systembenutzer, die für dynamische Authentifizierungsmodule verwendet werden, die Option **Für direkte Anmeldung gesperrt**. Damit wird eine

direkte Anmeldung an den One Identity Manager-Werkzeugen mit diesen Systembenutzern verhindert.

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 Berechtigungs- und Benutzeroberflächenstruktur können Sie eine Zuordnung von Funktionsgruppen zu Berechtigungsgruppen vornehmen. Über Funktionsgruppen bilden Sie die Funktionen der Personen in einem Unternehmen ab, beispielsweise IT Controller oder Niederlassungsleiter. Die Funktionsgruppen ordnen Sie den Berechtigungsgruppen zu. Eine Funktionsgruppe kann auf mehrere Berechtigungsgruppen verweisen und es können mehrere Funktionsgruppen auf eine Berechtigungsgruppe 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 Berechtigungsgruppen 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 Berechtigungsgruppe"
      />
      <Usermappings>
            <Usermapping
                  DialogUser = "Name des Systembenutzers"
                  Selection = "Auswahlkriterium"
            />
            ...
      </Usermappings>
</DialogUserDetect>
```

Verwandte Themen

- Beispiel für eine einfache Zuordnung zum Systembenutzer auf Seite 127
- Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 128
- Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 129
- Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen auf Seite 43

Beispiel für eine einfache Zuordnung zum Systembenutzer

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

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

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

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

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

Definieren Sie einen neuen Systembenutzer **dlg_all** und nehmen Sie diesen in die Berechtigungsgruppen **vi_DE-CentralPwd**, **vi_DE-ITShopOrder** und **WebShop_ Customer_Grp** auf.

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 125
- Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 128
- Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 129
- Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen auf Seite 43

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 Berechtigungen. Richten Sie einen neuen Systembenutzer **dlg_kst** ein und nehmen Sie diesen in die Berechtigungsgruppen **vi_DE-CentralPwd**, **vi_DE-ITShopOrder** und **WebShop_ Customer_Grp** auf. Dem Systembenutzer geben Sie zusätzlich die Sichtbarkeitsberechtigung und die Bearbeitungsberechtigung 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 125
- Beispiel für eine einfache Zuordnung zum Systembenutzer auf Seite 127
- Beispiel für eine Zuordnung über Funktionsgruppen auf Seite 129
- Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen auf Seite 43

Beispiel für eine Zuordnung über Funktionsgruppen

Für die Zuordnung von Funktionsgruppen zu Berechtigungsgruppen 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 Berechtigungsgruppen 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 Berechtigungsgruppen mit den notwendigen Berechtigungen ein.

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

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

```
<DialogUserDetect>
    <FunctionGroupMapping
        PersonToFunction = "custom_Person2Fu"
        FunctionToGroup = "custom_Fu2D"
    />
</DialogUserDetect>
```

Verwandte Themen

- Konfigurationsdaten zur dynamischen Ermittlung eines Systembenutzers auf Seite 125
- Beispiel für eine einfache Zuordnung zum Systembenutzer auf Seite 127
- Beispiel für eine Zuordnung zum Systembenutzer mittels Auswahlkriterium auf Seite 128
- Erteilen von Berechtigungen auf das One Identity Manager Schema über Berechtigungsgruppen auf Seite 43

Überprüfung der Authentifizierung

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

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

  Das Intervall können Sie über den Konfigurationsparameter **Common | Authentication | CheckInterval** anpassen. Bearbeiten Sie den Konfigurationsparameter im Designer.
- Die Anzahl der Sitzungen, die ein Benutzer innerhalb kurzer Zeit öffnen darf, ist begrenzt auf 10 Sitzungen in einer Minute.

Ist die Anzahl überschritten, erhält der Benutzer eine Fehlermeldung:

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

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

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

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

6

OAuth 2.0/OpenID Connect Authentifizierung

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 133
- OAuth 2.0/OpenID Connect Konfiguration erstellen auf Seite 134
- OAuth 2.0/OpenID Connect Konfiguration an Webanwendungen zuweisen auf Seite 140
- Aktivierende und deaktivierende Spalten für die Anmeldung festlegen auf Seite 142
- OAuth 2.0/OpenID Connect auf Seite 105
- OAuth 2.0/OpenID Connect (rollenbasiert) auf Seite 106
- Informationen für OAuth 2.0/OpenID Connect Authentifizierung aufzeichnen auf Seite 143
- OAuth 2.0/OpenID Connect Authentifizierung an der REST API des Anwendungsservers auf Seite 144

Ablauf der OAuth 2.0/OpenID Connect Authentifizierung

Die Webanwendung (oder Clientanwendung) fordert am Authorisierungsendpunkt den Autorisierungscode an. Über den Anmeldeendpunkt wird ein erweiterter Anmeldedialog aufgerufen, über den der Autorisierungscode ermittelt wird. Das Authentifzierungsmodul fordert ein Zugriffstoken vom Tokenendpunkt an. Zur Prüfung des Sicherheitstokens wird das Zertifikat herangezogen.

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

1. Konfiguration der OAuth 2.0/OpenID Connect Anwendung (Tabelle `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 134
- OAuth 2.0/OpenID Connect auf Seite 105
- OAuth 2.0/OpenID Connect (rollenbasiert) auf Seite 106

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:
        1. Wählen Sie **Automatische Konfigurationsdatenermittlung**.
        2. Geben Sie im Eingabefeld die Adresse (URL) für die automatische Ermittlung der Konfigurationsdaten an oder wählen Sie über das Pfeilmenü eine Beispieladresse.
        3. Klicken Sie **Ausführen**.
        4. Die Konfigurationsdaten werden ermittelt und in einen Dialogfenster anzeigt. Um die Konfigurationsdaten zu übernehmen, klicken Sie **OK**.
    - Wenn Sie die Konfigurationsdaten aus einer Vorlage erzeugen wollen:
        1. Wählen Sie **Aus einer Vorlagedatei erzeugen**.
        2. Klicken Sie **Auswählen** und wählen Sie die XML-Datei.

           Für den One Identity Redistributable STS (RSTS) wird die Datei mit einer Vorkonfiguration mitgeliefert. Die Datei `RSTS_Template.xml` finden Sie im One Identity Manager Installationsverzeichnis.
        3. Klicken Sie **Öffnen**.
    - 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 35: Allgemeine Konfigurationsdaten des Identitätsanbieters

Eigenschaft	Beschreibung
Anmeldeendpunkt	Uniform Resource Locator (URL) der erweiterten Anmeldeseite des Sicherheitstokendienstes. 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
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.
UserInfo-Endpunkt	URL des OpenID Connect UserInfo-Endpunktes.
Kein ID-Token Prüfung	Gibt an, ob eine Prüfung des ID-Tokens stattfindet. Ist die Option aktiviert, findet keine Überprüfung des ID-Tokens statt. Die Option kann nur bei einem Scope, der den Wert **openid** enthält, und einem besetzten UserInfo-Endpoint aktiviert werden.
Selbstsignierte Zertifikate zulässig	Gibt an, ob die Nutzung von selbstsignierten Zertifikaten bei der Verbindung zum Tokenend-

Eigenschaft	Beschreibung
	punkt und User Info-Endpunkt erlaubt ist.
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.
Angeforderte Referenzwerte der Authentifizierungskontextklasse	Leerzeichen-getrennte Zeichenfolge, die die acr-Werte angibt, welche der Autorisierungsserver für die Verarbeitung dieser Authentifizierungsanfrage verwenden soll, wobei die Werte in der Reihenfolge ihrer Präferenz erscheinen.

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 36: Informationen zum Zertifikat des Identitätsanbieters

Eigenschaft	Beschreibung
Zertifikatsendpunkt	Uniform Resource Locator (URL) des Zertifikatsendpunkts auf 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 37: 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) http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn Haben Sie die Konfigurationsdaten automatisch ermittelt, wählen Sie einen Wert aus der Liste.
Wert für Prüfung	Name des Claim-Typs, der zusätzlich geprüft werden soll. Der Claim-Typ muss unter genau diesem Namen im Token vorkommen. Mit der Prüfung wird sichergestellt, dass sich nur Personen anmelden können, in deren Token im angegebenen Claim-Typ genau der Vergleichswert enthalten ist.
Vergleichswert	Konkreter Wert des unter **Wert für Prüfung** angegebenen Claim-Typs, gegen den geprüft wird.

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 .

   Für die Anbindung mittels RSTS wählen Sie **RSTS-Client**. Einige der Informationen zur Anwendung **RSTS-Client** sind bereits vordefiniert.

b. Auf dem Tabreiter **Allgemein** erfassen Sie allgemeinen Informationen zur Anwendung.

Tabelle 38: Allgemeine Informationen zur Anwendung

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Anwendung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Client ID	ID der Anwendung beim Identitätsanbieter. Für Clientanwendungen 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
Weiterleitungs-URI nach Abmeldung senden	Angabe, die das Verhalten des Clients nach Abmelden von der Anwendung steuert. Zulässige Werte sind **Weiterleitungs-URI für die Anwendung senden** (Standard), **Keine Weiterleitungs-URI senden** und **Senden einer spezifischen Weiterleitungs-URI**.
Weiterleitungs-URI nach Abmeldung	URI, die nach dem Abmelden von der Anwendung versendet wird.
Standard	Gibt an, ob es sich um eine Standardanwendung für Clientanwendungen handelt.

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

Tabelle 39: Informationen zum Zertifikat der Anwendung

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

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

Tabelle 40: 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 privatem Schlüssel.

Eigenschaft	Beschreibung
Tokenendpunkt Zertifikat	Hexadezimaler Fingerabdruck des Zertifikates zur Prüfung des Tokens.
Angeforderte Referenzwerte der Authentifizierungskontextklasse	Leerzeichen-getrennte Zeichenfolge, die die acr-Werte angibt, welche der Autorisierungsserver für die Verarbeitung dieser Authentifizierungsanfrage verwenden soll, wobei die Werte in der Reihenfolge ihrer Präferenz erscheinen. Sind hier keine Referenzwerte definiert, werden die Referenzwerte des Identitätsanbieters verwendet.

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**.

Verwandte Themen

- One Identity Redistributable STS installieren auf Seite 157
- Multifaktor-Authentifizierung mit One Identity Defender auf Seite 149

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. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

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 134
- Aktivierende und deaktivierende Spalten für die Anmeldung festlegen auf Seite 142

Aktivierende und deaktivierende Spalten für die Anmeldung festlegen

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

Beachten Sie:

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

Beispiel:

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

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

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

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

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

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

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

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

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

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

Um festzulegen, welche Spalten ein Benutzerkonto für die Anmeldung aktivieren

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

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. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Informationen für OAuth 2.0/OpenID Connect Authentifizierung aufzeichnen

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

Um Informationen zur Authentifizierung im Protokoll auszuzeichnen

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

OAuth 2.0/OpenID Connect Authentifizierung an der REST API des Anwendungsservers

Die One Identity Manager REST API ist ein integraler Bestandteil des Anwendungsservers. Für die OAuth 2.0/OpenID Connect Authentifizierung an der REST API des Anwendungsservers, werden die Authentifizierungsmodule **OAuth2.0/OpenID Connect** und **OAuth2.0/OpenID Connect (rollenbasiert)** unterstützt.

Die Authentifizierung erfolgt über ein bereitgestelltes Zugriffstoken. Bei der ersten Anfrage mit einem neuen Zugriffstoken wird mit diesem Token und dem Authentifizierungsmodul eine Sitzung aufgebaut. Bei weiteren Zugriffen mit demselben Token wird dieselbe Sitzung benutzt. Dabei wird die Gültigkeitsdauer des Tokens überprüft.

Ausführliche Informationen zur One Identity Manager REST API finden Sie im *One Identity Manager REST API Reference Guide*.

Verwandte Themen

- Ablauf der OAuth 2.0/OpenID Connect Authentifizierung auf Seite 133
- OAuth 2.0/OpenID Connect Authentifizierung an der REST API einrichten auf Seite 144
- Authentifizierungsmodul für die OAuth 2.0/OpenID Connect Authentifizierung an der REST API auf Seite 145
- Authentifizierung externer Anwendungen über OAuth 2.0/OpenID Connect auf Seite 146

OAuth 2.0/OpenID Connect Authentifizierung an der REST API einrichten

HINWEIS: Um auf die REST API im Anwendungsserver zugreifen zu können, benötigen Benutzer die Programmfunktion **AppServer_API**.

Um die Authentifizierung an der REST API über OAuth 2.0/OpenID Connect einzurichten

- Aktivieren Sie im Designer den Konfigurationsparameter **QBM | AppServer | AccessTokenAuth**.
- Aktivieren Sie im Designer das jeweilige Authentifizierungsmodul **OAuth 2.0/OpenID Connect** oder **OAuth 2.0/OpenID Connect (rollenbasiert)**.
- Wenn das Authentifizierungsmodul **OAuth 2.0/OpenID Connect (rollenbasiert)** genutzt wird, aktivieren Sie zusätzlich den Konfigurationsparameter **QBM | AppServer | AccessTokenAuth | RoleBased**.
- Erstellen Sie im Designer die OAuth 2.0/OpenID Connect Konfiguration und weisen Sie die Konfiguration an die Webanwendung für den Anwendungsserver zu.
- Die URL für den Anwendungsserver muss bekannt sein.

  Bei der Installation des Anwendungsservers wird ein Eintrag für die Webanwendung mit der URL in der Tabelle `QBMWebApplication` erzeugt. Prüfen Sie, ob die URL (Spalte `BaseURL`) eingetragen ist.

Um die Einstellungen einer Webanwendung anzuzeigen

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Webserver Einstellungen**.
2. Wählen Sie im Listeneditor die Webanwendung.

Verwandte Themen

- OAuth 2.0/OpenID Connect Konfiguration erstellen auf Seite 134
- OAuth 2.0/OpenID Connect Konfiguration an Webanwendungen zuweisen auf Seite 140
- OAuth 2.0/OpenID Connect auf Seite 105
- OAuth 2.0/OpenID Connect (rollenbasiert) auf Seite 106
- Authentifizierungsmodule aktivieren auf Seite 117

Authentifizierungsmodul für die OAuth 2.0/OpenID Connect Authentifizierung an der REST API

Für die Authentifizierung über Zugriffstoken wird innerhalb des Anwendungsservers ein Authentifizierungsmodul bereitgestellt. Der Anwendungsserver-Client ermittelt mit den Informationen aus dem Authentifizierungsmodul das Zugriffstoken für die serverseitige Anmeldung.

Das Authentifizierungsmodul kann beispielsweise für Jobserver genutzt werden, die keine direkte Verbindung zur Datenbank haben, sondern gegen einen Anwendungsserver arbeiten.

Um das Authentifizierungsmodul zu nutzen, stellen Sie sicher, dass die Authentifizierung an der REST API über OAuth 2.0/OpenID Connect eingerichtet ist.

HINWEIS: Wenn eine Authentifizierung per Zugriffstoken erfolgt, dann ist die Nutzung anderer Authentifizierungsmodule ausgeschlossen und wird vom Anwendungsserver mit einem Fehler beantwortet.

Authentifizierungsdaten zum Aufbau einer Verbindung über die REST API des Anwendungsservers

```
Module=Token;Url=<URL des Anwendungsservers>;ClientId=<Client-
ID>;ClientSecret=<Secret>;TokenEndpoint=<Tokenendpunkt>
```

Mit folgenden Parametern:

- `URL`: URL des Anwendungsservers
- `ClientId`: Client-ID für die Authentifizierung am Tokenendpunkt
- `ClientSecret`: Secret-Wert für die Authentifizierung am Tokenendpunkt
- `TokenEndpoint`: URL des Tokenendpunktes

Ausführliche Informationen zum Erfassen von Verbindungsinformationen und Authentifizierungsdaten zum Anwendungsserver für Jobserver finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verwandte Themen

- OAuth 2.0/OpenID Connect Authentifizierung an der REST API einrichten auf Seite 144

Authentifizierung externer Anwendungen über OAuth 2.0/OpenID Connect

Um über externe Anwendungen auf die REST API im Anwendungsserver zuzugreifen, wird die Authentifizierung über die Authentifizierungsmodule **OAuth2.0/OpenID Connect** und **OAuth2.0/OpenID Connect (rollenbasiert)** unterstützt. Stellen Sie sicher, dass die Authentifizierung an der REST API über OAuth 2.0/OpenID Connect eingerichtet ist.

Um eine externe Anwendung über OAuth 2.0/OpenID Connect am One Identity Manager zu authentifizieren

1. Melden Sie sich beim externen Identitätsanbieter an, beispielsweise mit Redistributable STS (RSTS), und holen Sie das Zugriffstoken.

2. Stellen Sie sicher, dass das Token als Inhabertoken im Authentifizierungs-Header aller Anfragen übergeben wird.

HINWEIS: Die Sitzung muss bei der Anmeldung über ein Inhabertoken mittels eines Sitzungs-Cookies behandelt werden. Clients, die auf die REST API per Inhabertoken zugreifen, müssen also das beim ersten Zugriff vergebene Cookie aufbewahren und bei den nächsten Zugriffen mitschicken. Anderenfalls wird für jeden Zugriff eine neue Sitzung aufgebaut, was sehr viele Ressourcen kostet.

Verwandte Themen

- OAuth 2.0/OpenID Connect Authentifizierung an der REST API einrichten auf Seite 144
- OAuth 2.0/OpenID Connect auf Seite 105
- OAuth 2.0/OpenID Connect (rollenbasiert) auf Seite 106

Multifaktor-Authentifizierung im One Identity Manager

Für die Multifaktor-Authentifizierung an den One Identity Manager-Werkzeugen und dem Web Portal kann One Identity Defender genutzt werden. Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit One Identity Defender auf Seite 149.

Für Attestierungen oder die Entscheidung von Bestellungen kann die Multifaktor-Authentifizierung mit OneLogin eingerichtet werden. Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit OneLogin auf Seite 148.

Multifaktor-Authentifizierung mit OneLogin

Für bestimmte sicherheitskritische Aktionen im One Identity Manager kann die Multifaktor-Authentifizierung mit OneLogin eingerichtet werden. Diese kann beispielsweise für Attestierungen oder für die Entscheidung von Bestellungen im Web Portal genutzt werden. Jede Person, die diese Funktion nutzen möchte, muss mit einem OneLogin Benutzerkonto verbunden sein.

Voraussetzung

In OneLogin:

- Für alle Benutzerkonten, die für die Multifaktor-Authentifizierung genutzt werden sollen, ist mindestens eine Authentifizierungsmethode konfiguriert.

In One Identity Manager:

- Das OneLogin Modul ist vorhanden.

Um die Multifaktor-Authentifizierung für Attestierungen oder Bestellungen nutzen zu können

1. Richten Sie die Synchronisation mit einer OneLogin Domäne ein und starten Sie die Synchronisation.
2. Verbinden Sie Personen mit ihren OneLogin Benutzerkonten.
3. Konfigurieren Sie den API Server und das Web Portal für die Nutzung von OneLogin für die Multifaktor-Authentifizierung.
4. Richten Sie die Multifaktor-Authentifizierung für Attestierungen und Bestellungen im IT Shop ein.

Ausführliche Informationen finden Sie in den folgenden Handbüchern:

Thema	Handbuch
Einrichten und Starten der Synchronisation mit einer OneLogin Domäne	One Identity Manager Administrationshandbuch für die Anbindung von OneLogin Domänen
Konfiguration der Multifaktor-Authentifizierung in der Webanwendung	One Identity Manager Konfigurationshandbuch für Webanwendungen
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
Bestellung von Produkten, die eine Multifaktor-Authentifizierung benötigen	One Identity Manager Web Portal Anwenderhandbuch
Entscheiden von Bestellungen mit Multifaktor-Authentifizierung	
Attestierung mit Multifaktor-Authentifizierung	

Multifaktor-Authentifizierung mit One Identity Defender

Für die Multifaktor-Authentifizierung an den One Identity Manager-Werkzeugen und dem Web Portal kann One Identity Defender genutzt werden. Es wird ein Redistributable STS (RSTS) eingerichtet, um die Active Directory Authentifizierung über einen RADIUS Server bereitzustellen.

Voraussetzung

- One Identity Defender ist installiert und eingerichtet.

Um die Multifaktor-Authentifizierung über Defender einzurichten

1. Installieren Sie den RSTS.

   Im Installationsassistenten auf der Seite **Einstellungen für die Installation** erfassen Sie das Signatur-Zertifikat, die URL und das Konfigurationskennwort für die RSTS Administrationsoberfläche. Für Test- oder Demonstrationsumgebungen können Sie das Signatur-Zertifikat **Redistributable STS Demo** nutzen.
2. Konfigurieren Sie den RSTS.
3. Erstellen Sie eine OAuth 2.0/OpenID Connect Konfiguration.

   Dabei erstellen Sie einen neuen Identitätsanbieter. Diesen Identitätsanbieter benötigen Sie für die Konfiguration der Authentifizierung mit OAuth 2.0/OpenID Connect.
4. Konfigurieren Sie die Authentifizierung mit OAuth 2.0/OpenID Connect für das Web Portal.
5. Konfigurieren Sie die Authentifizierung mit OAuth 2.0/OpenID Connect für die One Identity Manager-Administrationswerkzeuge.
6. Testen Sie den Zugang zum Web Portal.
   - Nachdem Sie im Web-Browser die URL des Web Portals eingegeben haben, sollten Sie auf die Anmeldeseite des RSTS weitergeleitet werden.
   - Nach der Anmeldung mit Benutzername und Kennwort sollten Sie aufgefordert werden Ihren Defender Token einzugeben.

   Wenn beide Authentifizierungen erfolgreich waren, können Sie mit dem Web Portal arbeiten.
7. Testen Sie den Zugang zu den One Identity Manager-Administrationswerkzeugen.
   - Starten Sie ein Administrationswerkzeug, beispielsweise das Launchpad, und wählen Sie das Authentifizierungsverfahren **OAuth 2.0/OpenID Connect**.
   - Nach der Anmeldung mit Benutzername und Kennwort sollten Sie aufgefordert werden Ihren Defender Token einzugeben.

   Wenn beide Authentifizierungen erfolgreich waren, können Sie mit dem Administrationswerkzeug arbeiten.

Detaillierte Informationen zum Thema

- One Identity Redistributable STS installieren auf Seite 157
- RSTS für die Multifaktor-Authentifizierung konfigurieren auf Seite 151
- OAuth 2.0/OpenID Connect Konfiguration erstellen auf Seite 134
- Authentifizierung mit OAuth 2.0/OpenID Connect im Web Portal konfigurieren auf Seite 152
- Authentifizierung mit OAuth 2.0/OpenID Connect konfigurieren auf Seite 153

RSTS für die Multifaktor-Authentifizierung konfigurieren

Um die Multifaktor-Authentifizierung über einen RADIUS Server am RSTS zu konfigurieren

1. Starten Sie einen Web-Browser und rufen Sie die URL der RSTS Administrationsoberfläche auf.

   https://<Webanwendung>/RSTS/admin

   Nutzen Sie für die Anmeldung das bei der Installation vergebene Konfigurationskennwort.
2. Auf der Startseite wählen Sie **Authentication Providers**.
3. Auf der Seite **Authentication Providers** wählen Sie den Standard-Provider **Default Active Directory** und klicken Sie **Edit**.
4. Auf der Seite **Edit** wählen Sie den Tabreiter **Authentication Provider** und bearbeiten Sie die folgenden Einstellungen.
   - **Directory Type > Active Directory**: aktiviert
   - **Connection Information > Use Current Domain**: aktiviert
5. Wählen Sie den Tabreiter **Two Factor Authentication** und bearbeiten Sie die Einstellungen für Ihren Defender Security Server.
   - **Two Factor Authentication Settings > RADIUS**: aktiviert
   - **Server**, **Port**, **Shared Secret** und **Username Attribute**: Verbindungsinformationen zum RADIUS Server
   - (Optional) **Connection Information > Pre-authenticate For ChallengeResponse**: Verwendet den Antworttext des Defenders, anstelle des Standard-RADIUS-Antworttextes.
6. Wechseln Sie zur Startseite und wählen Sie **Applications**.
7. Auf der Seite **Applications** klicken Sie **Add Application**.
8. Auf der Seite **Edit** wählen Sie den Tabreiter **General Settings** und bearbeiten Sie die folgenden Einstellungen.
   - **Application Name**, **Authentication Provider**, **Realm/Client_ID/Issuer**, **Redirect Url**

   Die Weiterleitungs-URL für das Web Portal (**Redirect Url**) wird folgendermaßen gebildet: https://<Server>/<Application Name>/
9. Wählen Sie den Tabreiter **Certificates** und aktivieren Sie unter **Signing Certificate (Required)** das Signatur-Zertifikat, welches Sie bei der Installation des RSTS angegeben haben.

   Weitere Informationen finden Sie unter Multifaktor-Authentifizierung mit One Identity Defender auf Seite 149.
10. Klicken Sie **Finish**.

Verwandte Themen

- One Identity Redistributable STS installieren auf Seite 157

Authentifizierung mit OAuth 2.0/OpenID Connect im Web Portal konfigurieren

Um die Authentifizierung mit OAuth 2.0/OpenID Connect zu konfigurieren

1. Starten Sie den Web Designer.
2. Klicken Sie im Menü **Ansicht > Startseite**.
3. Klicken Sie auf der Startseite **Webanwendung auswählen** und wählen Sie die Webanwendung aus.
4. Klicken Sie **Einstellungen der Webanwendung bearbeiten**.
5. Im Dialogfenster **Einstellungen der Webanwendung bearbeiten** bearbeiten Sie die Einstellungen der Webanwendung.
   - **Authentifizierungsmodul**: Wählen Sie **OAuth 2.0/OpenID Connect (rollenbasiert)**.
   - **OAuth 2.0/OpenID Connect Konfiguration**: Wählen Sie den neu erstellten Identitätsanbieter.
   - **Client-ID für OAuth 2.0-Authentifizierung**: Wählen Sie die Client-ID, die Sie bei der Konfiguration des RSTS angegeben haben.
   - **Fingerabdruck des OAuth 2.0 Zertifikats**: Geben Sie den Fingerabdruck des Signatur-Zertifikats an, welches Sie bei der Konfiguration des RSTS ausgewählt haben.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Multifaktor-Authentifizierung mit One Identity Defender auf Seite 149
- RSTS für die Multifaktor-Authentifizierung konfigurieren auf Seite 151
- Authentifizierung mit OAuth 2.0/OpenID Connect konfigurieren auf Seite 153
- OAuth 2.0/OpenID Connect Konfiguration erstellen auf Seite 134

Authentifizierung mit OAuth 2.0/OpenID Connect konfigurieren

Um die Authentifizierung mit OAuth 2.0/OpenID Connect zu konfigurieren

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > OAuth 2.0/OpenID Connect Konfiguration**.
2. Wählen Sie im Listeneditor den neu erstellten Identitätsanbieter.
3. Wählen Sie den Tabreiter **Allgemein** und prüfen Sie die allgemeinen Konfigurationsdaten des Identitätsanbieters.
    - **Spalte für die Suche**: Wählen Sie **ADSAccount - ObjectGUID**.
4. Wählen Sie den Tabreiter **Anwendungen** und prüfen Sie die Konfiguration der OAuth 2.0/OpenID Connect Anwendung.
    - **Standard**: aktiviert
    - **Weiterleitungs-URI**: Wenn Sie die Multifaktor-Authentifizierung mit den Administrationswerkzeugen des One Identity Manager nutzen wollen, erfassen Sie **urn:InstalledApplication**.
5. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Multifaktor-Authentifizierung mit One Identity Defender auf Seite 149
- Authentifizierung mit OAuth 2.0/OpenID Connect im Web Portal konfigurieren auf Seite 152
- RSTS für die Multifaktor-Authentifizierung konfigurieren auf Seite 151
- OAuth 2.0/OpenID Connect Konfiguration erstellen auf Seite 134

Abgestufte Berechtigungen für SQL Server und Datenbank

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

In der Regel müssen die Benutzer und Berechtigungen nicht bearbeitet werden.

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

Verwandte Themen

- Anmeldungen für den Datenbankserver anzeigen auf Seite 154
- Berechtigungsebene des Benutzers anzeigen auf Seite 155
- Berechtigungen der Serverrollen und der Datenbankrollen anzeigen auf Seite 155
- Minimale Berechtigungsebenen der One Identity Manager-Werkzeuge auf Seite 163

Anmeldungen für den Datenbankserver anzeigen

Um Informationen für eine Anmeldung anzuzeigen

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Datenbankserverberechtigungen > Datenbankserver-Anmeldungen**.
2. Wählen Sie die Datenbankserver-Anmeldung. Es werden folgende Informationen werden abgebildet:

- **Anmeldename**: SQL Server Anmeldung des Benutzers.
- **Datenbankbenutzer**: Name des Datenbankbenutzers.
- **Berechtigungsebene**: Berechtigungsebene der Anmeldung. Es werden die Berechtigungsebenen **Endbenutzer**, **Konfigurationsbenutzer**, **Administrativer Benutzer**, **Systemadministrator** und **Unbekannt** abgebildet.

3. Um die zugewiesenen Datenbankrollen und Serverrollen anzuzeigen, wählen Sie den Tabreiter **Datenbank- oder Serverrolle**.

Berechtigungsebene des Benutzers anzeigen

HINWEIS:

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

Um die Berechtigungsebene für den angemeldeten Benutzer zu ermitteln

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

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

Verwandte Themen

- Anmeldungen für den Datenbankserver anzeigen auf Seite 154

Berechtigungen der Serverrollen und der Datenbankrollen anzeigen

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

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

Um die Berechtigungen der Serverrollen und Datenbankrollen anzuzeigen

- Wählen Sie im Designer in der Kategorie **Basisdaten > Sicherheitseinstellungen > Datenbankserverberechtigungen > Datenbank- und Serverrollen** die Serverrolle oder die Datenbankrolle.

  Im Listeneditor werden die einzelnen Berechtigungen angezeigt.

One Identity Redistributable STS installieren

Der Redistributable STS (RSTS) ist ein Secure Token Server-Komponentendienst, der die Benutzerauthentifizierung unter Verwendung von Standard-Föderationsprotokollen wie WS-Federation und OAuth 2.0 bereitstellen soll. One Identity Manager nutzt den RSTS für die Authentifizierung an Webanwendungen mit Webauthn und OAuth 2.0.

Ausführliche Informationen zur Webauthn-Konfiguration finden Sie im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Um den RSTS zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Wechseln Sie auf den Tabreiter **Andere Produkte**.
3. Wählen Sie **One Identity Redistributable STS** und klicken Sie **Installieren**.
4. Auf der Startseite des Installationsassistenten klicken Sie **Weiter**.
5. Auf der Seite **Datenbank auswählen** wählen Sie die One Identity Manager-Datenbankverbindung. Verwenden Sie zur Anmeldung einen Benutzer, der mindestens administrative Berechtigungen auf die Datenbank hat.
6. Auf der Seite **Einstellungen für die Installation** erfassen Sie alle erforderlichen Informationen.
7. Auf der Seite **Installation** sehen den Installationsfortschritt. Wenn die Installation beendet ist, klicken Sie **Weiter**.
8. Um den Installationsassistenten zu beenden, klicken Sie **Fertig**.

Verwandte Themen

- OAuth 2.0/OpenID Connect auf Seite 105
- OAuth 2.0/OpenID Connect Authentifizierung auf Seite 132
- Multifaktor-Authentifizierung mit One Identity Defender auf Seite 149

Blind SQL-Injection verhindern

Aus Sicherheitsgründen können von den Frontends und Webanwendungen keine direkten Datenbankanfragen ausgeführt werden. Definierte SQL-Operatoren werden mit einem Risiko bewertet, so dass diese nicht über die One Identity Manager-Komponenten verwendet werden können. Dazu gehören beispielsweise `LIKE`, `NOT LIKE`, `<`, `<=`, `>` oder `>=`.

Um bestimmte Funktionen in den One Identity Manager-Komponenten weiterhin nutzen zu können, benötigen die Benutzer die Programmfunktion **Common_AllowRiskyWhereClauses**.

Benutzer, die diese Programmfunktion nicht besitzen, können nur Datenbankabfragen ausführen, die als vertrauenswürdig eingestuft sind oder kein Risiko darstellen (Risikowert = **0,0**). Einige der Funktionen in den One Identity Manager-Komponenten, wie beispielsweise das Testen von dynamischen Rollen oder die Ausführung von Filterabfragen, sind ohne die Programmfunktion nicht möglich.

Soll es bestimmten Benutzern möglich sein, sicherheitskritische Abfragen auszuführen, können Sie die Berechtigungen über Berechtigungsgruppen an die Benutzer vergeben.

- Für die nicht-rollenbasierte Anmeldung wird die Berechtigungsgruppe **QBM_Critical_WhereClause** bereitgestellt. Diese Gruppe besitzt die Programmfunktion. Nehmen Sie die Systembenutzer, die sicherheitskritische Abfragen ausführen dürfen, in die Berechtigungsgruppe auf. Administrative Systembenutzer erhalten diese Berechtigungsgruppe automatisch.
- Für die rollenbasierte Anmeldung wird die Berechtigungsgruppe **QER_4_Critical_WhereClause** bereitgestellt. Diese Gruppe besitzt die Programmfunktion. Die Berechtigungsgruppe ist mit der Anwendungsrolle **Basisrollen | Sicherheitskritische Abfragen** verbunden. Nehmen Sie die Personen, die sicherheitskritische Abfragen ausführen dürfen, in die Anwendungsrolle auf.

Mit welchem Risiko die Ausführung von SQL-Anweisungen bewertet wird, können Sie zusätzlich über Konfigurationsparameter steuern.

HINWEIS: Die Konfigurationsparameter wirken nur für Benutzer, die die Programmfunktion **Common_AllowRiskyWhereClauses** besitzen.

- Über den Konfigurationsparameter **QBM | SQLCheck | RiskEvaluation** legen Sie die Risikobewertung der ausgeführten SQL-Anweisungen fest. Zulässige Werte sind:

- **Low**: SQL-Anweisungen mit gewissem Risiko sind zulässig.
- **Medium**: Das Risiko von SQL-Anweisungen wird in abgeschwächter Höhe bewertet. Somit wird der Schwellwert zur Sperrung des Benutzers später erreicht und es sind mehr Abfragen möglich.
- **Strict**: Das Risiko von SQL-Anweisungen wird in voller Höhe bewertet. Eine Sperrung des Benutzers erfolgt aber erst nach Erreichen eines gewissen Schwellwertes.

Ist der Konfigurationsparameter nicht aktiviert, erfolgt die Risikobewertung mit dem Wert **Strict**.

- Über den Konfigurationsparameter **QBM | SQLCheck | SubSelect** legen Sie fest, wie die Bewertung von SQL-Anweisungen mit Unterabfragen erfolgen soll. Ist der Konfigurationsparameter aktiviert, werden Fundstellen in SQL-Anweisungen mit Unterabfragen als höheres Risiko eingestuft.

Hinweise für kundenspezifische Anpassungen

- Datenbankabfragen, die beispielsweise auf kundenspezifischen Formularen benötigt werden oder Datenbankabfragen, die über die API des Anwendungsservers ausgeführt werden, müssen im One Identity Manager als vordefinierte Datenbankabfragen formuliert werden. Die Ausführung der Datenbankabfragen erfolgt immer mit den Berechtigungen des angemeldeten Benutzers. Ausführliche Informationen zum Verwenden vordefinierter Datenbankabfragen finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Beispiele für die Verwendung von vordefinierten Datenbankabfragen finden Sie auf dem Installationsmedium im Verzeichnis `QBM\dvd\AddOn\ApiSamples`.
- Für die alphabetische Darstellung von beispielsweise Personen oder Unternehmensstrukturen können Sie in kundenspezifischen Menüanpassungen die Tabelle `QERVFirstUnicodeChar` nutzen.

Anhang A

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

Tabelle 41: Programmfunktionen zum Starten der One Identity Manager-Werkzeuge

Programmfunktion	Beschreibung
ApplicationStart_ Analyzer	Erlaubt das Starten des Programms Analyzer (`Analyzer.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`).

Programmfunktion	Beschreibung
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`).
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`.

Programmfunktion	Beschreibung
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 Berechtigungsgruppen zuweisen auf Seite 74
- Systembenutzer in Berechtigungsgruppen aufnehmen auf Seite 59
- Personen an Anwendungsrollen zuweisen auf Seite 35

Anhang B

Minimale Berechtigungsebenen der One Identity Manager-Werkzeuge

HINWEIS:

- Verbindungen, die nicht die erwartete Berechtigungsebene für SQL Server-Anmeldungen verwenden, werden nicht im Verbindungsdialog angezeigt.
- Wenn Sie im Verbindungsdialog eine vorhandene Datenbankverbindung wählen, wird die Berechtigungsebene der verwendeten Anmeldung im Tooltipp angezeigt.

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

Tabelle 42: Berechtigungsebenen der One Identity Manager-Werkzeuge

Werkzeug	Minimale Berechtigungsebene
Analyzer	Endbenutzer
Anwendungsserver	Endbenutzer oder Konfigurationsbenutzer (abhängig von der Aufgabe des Anwendungsservers)
API Server	Endbenutzer
Configuration Wizard	Administrativer Benutzer
Crypto Configuration	Konfigurationsbenutzer
Data Import	Endbenutzer Konfigurationsbenutzer (Speichern der Importdefinition)
Database Transporter	Konfigurationsbenutzer
Database Compiler	Konfigurationsbenutzer
DBClone	Administrativer Benutzer
DBComparer	Konfigurationsbenutzer

Werkzeug	Minimale Berechtigungsebene
Designer	Konfigurationsbenutzer Einige Konsistenzprüfungen benötigen die Berechtigungsebene für administrative Benutzer.
Job Queue Info	Konfigurationsbenutzer
Launchpad	Endbenutzer Einige der Anwendungen, die aus dem Launchpad gestartet werden, benötigen abweichende Berechtigungsebenen.
License Meter	Endbenutzer
Manager	Endbenutzer Einige Funktionen benötigen die Berechtigungsebene für Konfigurationsbenutzer, beispielsweise das Öffnen der Synchronisationsprojekte für Zielsysteme. Einige Konsistenzprüfungen benötigen die Berechtigungsebene für Konfigurationsbenutzer oder administrative Benutzer.
Object Browser	Endbenutzer
One Identity Manager Service	Konfigurationsbenutzer für die Prozessabholung über **MSSQLJobProvider**
Report Editor	Konfigurationsbenutzer
Schema Extension	Konfigurationsbenutzer
Server Installer	Konfigurationsbenutzer
Software Loader	Konfigurationsbenutzer
Synchronization Editor	Konfigurationsbenutzer
System Debugger	Konfigurationsbenutzer
Web Designer	Konfigurationsbenutzer
Web Designer Configuration Editor	Konfigurationsbenutzer
Web Portal	Endbenutzer
Kennwortrücksetzungsportal	Endbenutzer
Web Portal für Betriebs-unterstützung	Endbenutzer
AppServer.Installer.CMD.exe	Konfigurationsbenutzer

Werkzeug	Minimale Berechtigungsebene
AutoUpdate.exe	Konfigurationsbenutzer
DBCompilerCMD.exe	Konfigurationsbenutzer
DBConsCheckCmd.exe	Endbenutzer Einige Konsistenzprüfungen benötigen die Berechtigungsebene für Konfigurationsbenutzer oder administrative Benutzer.
DataImporterCMD.exe	Endbenutzer
DBTransporterCMD.exe	Konfigurationsbenutzer
Quantum.MigratorCmd.exe	Administrativer Benutzer
SchemaExtensionCmd.exe	Konfigurationsbenutzer
SoftwareLoaderCMD.exe	Konfigurationsbenutzer
VI.WebDesigner.CompilerCmd.exe	Konfigurationsbenutzer
WebDesigner.InstallerCMD.exe	Konfigurationsbenutzer

Verwandte Themen

- Abgestufte Berechtigungen für SQL Server und Datenbank auf Seite 154

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

A

B

D

E

L

M

O

P

R

S

T

Z