One Identity Manager 9.1.3

Installationshandbuch

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

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

One Identity Manager Installationshandbuch
Aktualisiert - 29. April 2024, 12:22 Uhr

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

Inhalt

1

Über dieses Handbuch

Das *One Identity Manager Installationshandbuch* beschreibt die Installation und erste Inbetriebnahme des One Identity Manager. Sie erhalten einen Überblick über die Architektur des One Identity Manager und über die Funktionen der verschiedenen One Identity Manager-Werkzeuge. Sie erhalten Informationen darüber, welche Voraussetzungen Sie zur Installation des One Identity Manager benötigen, wie Sie die Komponenten des One Identity Manager einrichten, installieren und aktualisieren.

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

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

Verfügbare Dokumentation

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

Überblick über den One Identity Manager

One Identity Manager vereinfacht konzernweit den Prozess der Verwaltung von Benutzeridentitäten, Zugriffsberechtigungen und Sicherheitsrichtlinien. Sie ermöglichen den Unternehmen die Kontrolle über Identitätsverwaltung und Zugriffsentscheidungen, während sich die IT-Teams auf ihre Kernkompetenzen fokussieren können.

Mit diesen Produkten können Sie:

- Gruppenverwaltung mittels Selbstbedienung und Attestierung für Active Directory mit der One Identity Manager Active Directory Edition umsetzen,
- Zugriffsentscheidungen für unstrukturierte Daten mit der One Identity Manager Data Governance Edition vereinfachen,
- Access Governance Anforderungen in Ihrem gesamten Konzern plattformübergreifend mit dem One Identity Manager verwirklichen.

Jedes dieser Szenarien-spezifischen Produkte basiert auf der selben prozessoptimierten Architektur und realisiert, im Gegensatz zu "traditionellen" Lösungen, die wesentlichen Identity- und Access Management Herausforderungen mit einem Bruchteil an Komplexität, Zeitaufkommen und Kosten.

One Identity Starling

Starten Sie Ihr Abonnement in Ihrem One Identity On-Prem-Produkt und verbinden Sie Ihre On-Prem-Lösungen mit unserer Cloud-Plattform One Identity Starling. Ermöglichen Sie Ihrem Unternehmen den sofortigen Zugriff auf eine Reihe von in der Cloud bereitgestellten Microservices, die die Funktionen Ihrer On-Prem-Lösungen von One Identity erweitern. Wir werden One Identity Starling ständig neue Produkte und Funktionen zur Verfügung stellen. Eine kostenlose Testversion unserer One Identity Starling-Angebote sowie die neuesten Produktfeatures erhalten Sie unter cloud.oneidentity.com.

Editionen des One Identity Manager

Der One Identity Manager ist in folgenden Editionen verfügbar.

One Identity Manager

Die Edition enthält alle Management Module (IT Shop & Workflow, Delegation, Verwaltung von Systemrollen und Geschäftsrollen, Role Mining, Risikobewertung, Attestierung, Compliance, Unternehmensrichtlinien, Abonnements von Berichten) sowie den Unified Namespace und Konnektoren für Active Directory.

One Identity Manager Active Directory Edition

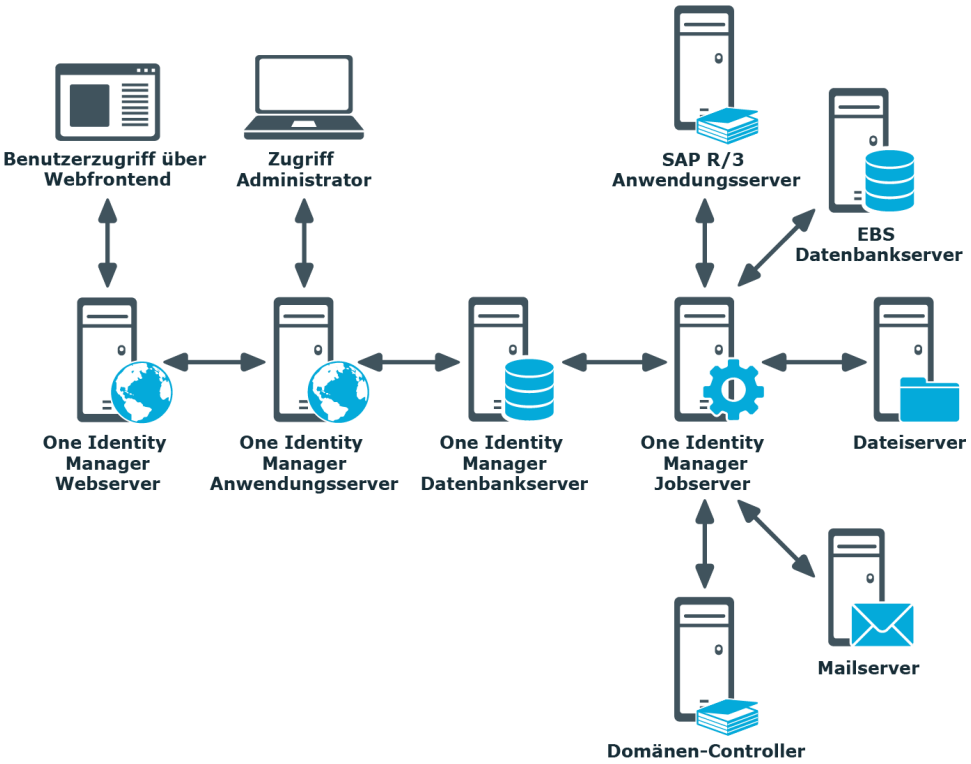
Die Edition enthält alle erforderlichen Funktionen für die Active Directory Unterstützung inklusive Konnektoren für Active Directory , Attestierung, IT Shop & Workflow und Berichtsfunktionen.

One Identity Manager Data Governance Edition

Die Edition enthält alle erforderlichen Funktionen für die Data Governance Unterstützung inklusive Konnektoren für Active Directory und SharePoint , Risikobewertung, Attestierung, Compliance, Unternehmensrichtlinien, Delegierung, Abonnements von Berichten und den Data Governance Dienst.

Architektur des One Identity Manager

Abbildung 1: Überblick über die Komponenten des One Identity Manager



Der One Identity Manager besteht aus folgenden Komponenten.

Datenbank

Die Datenbank stellt den Kern des One Identity Manager dar. Sie erfüllt die Hauptaufgaben der Datenhaltung und der Berechnung von Vererbungen. Vererbt werden können Eigenschaften von Objekten entlang von hierarchischen Strukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Bei der Datenhaltung bildet die Datenbank die zu verwaltenden Zielsysteme, die ERP-Strukturen sowie Regeln zur Compliance und Zugriffsberechtigungen ab.

Logisch ist die Datenbank in die zwei Bereiche der Nutzdaten und der Metadaten geteilt. Die Nutzdaten enthalten alle für die Datenpflege nötigen Informationen wie beispielsweise Informationen über Personen, Benutzerkonten, Gruppen, Mitgliedschaften und Betriebsdaten, Genehmigungsworkflows, Attestierungen, Rezertifizierungen und Complianceregeln.

Die Metadaten enthalten die Beschreibung des Anwendungsdatenmodell sowie Skripte für Format- und Bildungsvorschriften oder bedingte Wechselwirkungen. Die komplette Systemkonfiguration des One Identity Managers, die gesamten Einstellungen zur Steuerung der Frontends und die Queues für asynchrone Verarbeitung der Daten und Prozesse sind ebenfalls Teil der Metadaten.

Die Neuberechnung von Vererbungen wird durch die Triggerlogik der Datenbank ausgelöst. Die Trigger stellen dazu Verarbeitungsaufträge in eine als DBQueue bezeichnete Auftragsliste ein. Der DBQueue Prozessor verarbeitet diese Aufträge und berechnet die Vererbungen der jeweiligen Datenbankobjekte neu. Eine als Jobqueue bezeichnete Tabelle dient der Ablage von Verarbeitungsaufträgen, die von der Objektschicht auszuführen sind.

Als Datenbanksystem kommt SQL Server oder eine verwaltete Instanz in Azure SQL-Datenbank zum Einsatz.

Serverdienst

Der One Identity Manager verwendet zur Abbildung von Geschäftsprozessen sogenannte Prozesse. Ein Prozess besteht aus Prozessschritten, die Verarbeitungsaufgaben darstellen und über Vorgänger-Nachfolger-Beziehungen miteinander verbunden sind. Dieses Funktionsprinzip erlaubt es, flexibel Aktionen und Abläufe an die Ereignisse von Objekten zu koppeln. Die Modellierung der Prozesse erfolgt über Prozessvorlagen. Die Umwandlung der als Skript definierten Vorlagen in Prozessen und Prozessschritten in einen konkreten Prozess in der Jobqueue übernimmt der Jobgenerator.

Der One Identity Manager Service sorgt für die Verbreitung der in der One Identity Manager-Datenbank verwalteten Informationen im Netzwerk. Der One Identity Manager Service übernimmt die Datensynchronisation zwischen Datenbank und den angebundenen Zielsystemen sowie die Durchführung von Aktionen auf Datenbank- und Dateiebene.

Der One Identity Manager Service holt die Prozessschritte aus der Jobqueue ab. Die Prozessschritte werden von Prozesskomponenten ausgeführt. Der One Identity Manager Service erzeugt dazu eine Instanz der benötigten Prozesskomponente und übergibt die Parameter des Prozessschrittes. Eine Entscheidungslogik überwacht die Ausführung der Prozessschritte und veranlasst abhängig vom gemeldeten Ausführungsergebnis die weitere Verarbeitung des Prozesses. Der One Identity Manager Service ermöglicht die parallele Verarbeitung von Prozessschritten, da er mehrere Instanzen von Prozesskomponenten erzeugen kann.

Der One Identity Manager Service ist die einzige Komponente des One Identity Manager, die berechtigt ist, Änderungen in den Zielsystemen auszuführen.

Anwendungsserver

Die Clients verbinden sich zu einem Anwendungsserver, der die Geschäftslogik hält. Der Anwendungsserver stellt einen Verbindungspool für den Zugriff auf die Datenbank zur Verfügung und sorgt für eine sichere Verbindung zur Datenbank. Die Clients senden ihre Anfragen an den Anwendungsserver, dieser führt die Verarbeitung der Objekte wie beispielsweise die Bildung von Werten nach definierten Bildungsregeln aus und sendet die Ergebnisse an die Clients zurück. Mit dem Speichern eines Objektes werden die Daten vom Anwendungsserver an die Datenbank übergeben.

Die Clients können alternativ ohne externen Anwendungsserver arbeiten und selbst die Objektschicht halten und direkt auf die Datenbankschicht zugreifen. In den Clients kommt in diesem Fall nur der Teil der Objektschicht zum Einsatz, der die Erfassungsprozesse abbildet.

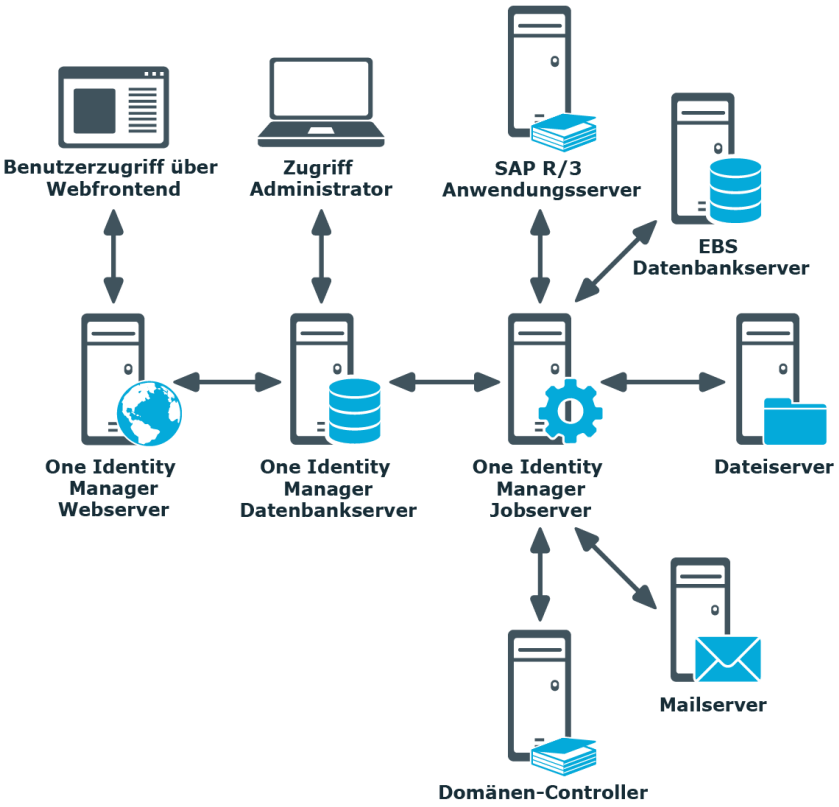
Webserver

Für den Einsatz browserbasierter Frontends wird auf einem Webserver eine Applikation betrieben, die aus einer Renderengine für Webseiten besteht. Der Benutzer greift mittels eines Webbrowsers auf die für ihn dynamisch erstellte und angepasste Website zu. Der Austausch zwischen Datenbank und Webserver kann über den Anwendungsserver oder direkt erfolgen.

Frontends

Für unterschiedliche Aufgabenstellungen gibt es verschiedene Frontends. Beispielsweise wird zur Konfiguration des One Identity Manager ein anderes Frontend verwendet als zur Verwaltung von Personendaten. Die darzustellenden Inhalte und ihre Änderbarkeit werden in Abhängigkeit der Zugriffsberechtigungen des jeweiligen Benutzers durch die Objektschicht bestimmt. Als Frontends stehen sowohl Clients als auch eine browserbasierte Lösung zur Verfügung.

Abbildung 2: Überblick über die Komponenten des One Identity Manager ohne Anwendungsserver



Verwandte Themen

- Werkzeuge des One Identity Manager auf Seite 14
- Welche Komponenten und Frontends arbeiten mit einem Anwendungsserver? auf Seite 20

Werkzeuge des One Identity Manager

Für unterschiedliche Aufgabenstellungen gibt es verschiedene Werkzeuge. Beispielsweise wird zur Konfiguration des One Identity Manager ein anderes Werkzeuge verwendet als zur Verwaltung von Personendaten. Die darzustellenden Inhalte und ihre Änderbarkeit sind abhängig von den Berechtigungen des angemeldeten Benutzers.

Tabelle 1: Übersicht der One Identity Manager-Werkzeuge

Werkzeug	Kurzbeschreibung
Launchpad	Das Launchpad ist das zentrale Werkzeug zum Starten der Administrationswerkzeuge und Konfigurationswerkzeuge des One Identity Manager. Mit dem Launchpad können Sie die vorhandene One Identity Manager Installation prüfen und die Werkzeuge des One Identity Manager zur Ausführung einzelner Aufgaben starten. Das Launchpad ist kundenspezifisch erweiterbar. Sie können im Designer eigene Menüeinträge und Aktionen für das Launchpad definieren.
Web Portal	Das Web Portal ist eine webbasierte Applikation für alle One Identity Manager Benutzer. Das Web Portal stellt die stringente Arbeitsabläufe in folgenden Bereichen bereit: • Eigene Personenstammdaten und eigenes Kennwort ändern. • Personenstammdaten für untergeordnete Mitarbeiter bearbeiten oder neu erfassen. • Produkte im IT Shop suchen, bestellen, abbestellen oder verlängern. • Eigene Rollen delegieren. • Zugewiesene Entscheidungen, Attestierungsvorgänge und Regelverletzungen bearbeiten. Im Infosystem erhalten Sie verschiedene Auswertungen, zum Beispiel über eigene Bestellvorgänge oder

Werkzeug	Kurzbeschreibung
	Attestierungsvorgänge, Mitarbeiterzahlen, Genehmigungen, Regelverletzungen oder den Unified Namespace. Das Web Portal wird über den API Server bereitgestellt. Der Benutzer greift mittels eines Webbrowsers auf die für ihn dynamisch erstellte und angepasste Website zu. Aus Kompatibilitätsgründen zu früheren Versionen wird das Web Designer Web Portal bereitgestellt. Das Web Designer Web Portal benötigt einen Webserver.
Kennwortrücksetzungsportal	Das Kennwortrücksetzungsportal ermöglicht den Benutzern das sichere Zurücksetzen von Kennwörtern für die von ihnen verwalteten Benutzerkonten. Das Kennwortrücksetzungsportal wird über den API Server bereitgestellt. Die erforderliche Sicherheit wird durch die Multifaktor-Authentifizierung gewährleistet.
Web Portal für Betriebs-unterstützung	Das Web Portal für Betriebsunterstützung unterstützt Sie bei der Verwaltung und beim Betrieb Ihrer Webanwendungen. Mit dem Web Portal für Betriebsunterstützung überwachen Sie die Verarbeitung von Prozessen und DBQueue-Aufträgen. Zusätzlich können Sie Zugangscodes für Ihre Mitarbeiter erzeugen. Das Web Portal für Betriebsunterstützung wird über den API Server bereitgestellt.
Manager	Der Manager ist das zentrale Administrationswerkzeug zur Einrichtung aller Informationen über Personen und ihre Identitäten. Es werden alle Informationen abgebildet und bearbeitet, die zur Verwaltung von Personen mit ihren Benutzerkonten, Berechtigungen und unternehmensspezifischen Rollen in einem One Identity Manager-Netzwerk erforderlich sind. Unternehmensressourcen, die die Mitarbeiter für ihre Arbeit benötigen, können erfasst und den Personen zugewiesen werden. Nutzen Sie den Manager außerdem, um • unternehmensspezifische IT-Richtlinien zu definieren, • einen IT Shop einzurichten, über den Unternehmensressourcen und Zuweisungen bestellt werden, • spezielle Genehmigungsverfahren einzurichten,

Werkzeug	Kurzbeschreibung
	mit denen Bestellungen autorisiert und die Einhaltung der IT-Richtlinien überprüft werden, • Attestierungsverfahren einzurichten, mit denen die Korrektheit der Informationen über Personen oder Rollen und ihre Zuweisungen regelmäßig attestiert werden. Durch den Einsatz von One Identity Manager Anwendungsrollen erhält jeder One Identity Manager Benutzer nur die Berechtigungen, die er zur Erfüllung seiner administrativen Aufgaben benötigt. Die Funktionen des Manager können als Webanwendung bereitgestellt werden.
Synchronization Editor	Die Anbindung verschiedener Zielsysteme an den One Identity Manager wird mit dem Synchronization Editor realisiert. Mit diesem Werkzeug konfigurieren Sie die Synchronisation von Daten beliebiger Zielsysteme und legen fest, welche Daten der Zielsysteme in der One Identity Manager-Datenbank abgebildet werden. Dazu definieren Sie das Mapping der Objekteigenschaften und den Ablauf der Synchronisation als Workflow.
Analyzer	Mit dem Analyzer können Sie Datenkorrelationen in der Datenbank automatisch analysieren und erkennen. Diese Informationen können genutzt werden, um zum Beispiel direkte Berechtigungszuordnungen durch indirekte Zuordnungen zu ersetzen, und somit den Verwaltungsaufwand zu reduzieren.
Job Queue Info	Job Queue Info unterstützt Sie bei der Kontrolle des aktuellen Zustandes der in einem One Identity Manager-Netzwerk laufenden Dienste. Es ermöglicht eine detaillierte und übersichtliche Darstellung der Aufträge in der JobQueue und stellt verschiedene Abfragen des One Identity Manager Service auf den Servern zur Verfügung. Das Werkzeug liefert Zustandsinformationen im laufenden Betrieb und ermöglicht eine schnelle Fehlererkennung und Fehlersuche.
Configuration Wizard	Der Configuration Wizard ist das Werkzeug mit dem die Datenbank auf einem SQL Server für die Verwendung in einem One Identity Manager-Netzwerk eingerichtet wird. Mit dem Configuration Wizard werden die benötigten Tabellen, Datentypen, Datenbankprozeduren des One Identity Manager Schemas in die Datenbank eingespielt. Die SQL Server Anmeldungen und Datenbankbenutzer

Werkzeug	Kurzbeschreibung
	mit den Berechtigungen auf das One Identity Manager Schema werden angelegt. Im One Identity Manager ist eine automatische Versionsverwaltung integriert, die einen konsistenten Stand der Bestandteile des One Identity Manager untereinander als auch zur Datenbank sichert. Werden Erweiterungen implementiert, die die Struktur verändern (zum Beispiel Tabellenerweiterungen), ist eine Migration der Datenbank erforderlich. Der Configuration Wizard führt diese Schemainstallation in Abhängigkeit vom aktuellen Stand des Schemas durch.
Designer	Der Designer ist das zentrale Werkzeug zur Konfiguration des One Identity Manager. Das Programm bietet einen Überblick über das gesamte Datenmodell des One Identity Manager. Es ermöglicht die Konfiguration globaler Systemeinstellungen, wie beispielsweise Sprachen oder Konfigurationsparametern sowie die Anpassung der Benutzeroberfläche der unterschiedlichen Administrationswerkzeuge. Mit dem Designer können Sie die Berechtigungen für die verschiedenen administrativen Aufgaben der einzelnen Anwender und Anwendergruppen festlegen. Eine weitere zentrale Aufgabe ist die Definition von Arbeitsabläufen zur technischen Abbildung der Administrationsprozesse in einem Unternehmen. Der Designer stellt für die Systemkonfiguration des One Identity Manager verschiedene Editoren zur Verfügung. Funktionsumfang und Arbeitsweise der Editoren sind abgestimmt auf die unterschiedlichen Konfigurationsanforderungen.
Web Designer	Der Web Designer ist das Werkzeug zur Konfiguration und Erweiterung des Web Designer Web Portals. Er stellt Funktionen zur Verfügung, mit denen die Arbeitsabläufe des Web Designer Web Portals angepasst und neue Arbeitsabläufe entwickelt werden.
Data Import	Mit dem Programm Data Import bietet der One Identity Manager einen einfache Möglichkeit für den Datenimport aus anderen Systemen. Nutzen Sie das Programm, um Daten betrieblicher Ressourcen aus externen Quellen in Ihre Datenbank zu importieren. Das Programm unterstützt Importe aus Dateien und direkte Importe aus anderen Datenbanksystemen. Datenimporte können sofort ausgeführt werden. Zusätzlich werden Importskripte erzeugt, mit denen Datenimporte über

Werkzeug	Kurzbeschreibung
	kundenspezifische Prozesse ausführbar sind. Die Importdefinition wird gespeichert und kann bei weiteren Datenimporten genutzt werden.
Crypto Configuration	Unter Umständen ist es notwendig, Informationen verschlüsselt in der Datenbank abzulegen. Die Verschlüsselung erfolgt mit dem Programm Crypto Configuration. Das Programm erzeugt eine Schlüsseldatei und konvertiert die Inhalte der betroffenen Datenbankspalten. Die Schlüsselinformationen werden in der Datenbank abgelegt.
Database Compiler	Nach Änderungen von Konfigurationsdaten müssen Sie die One Identity Manager-Datenbank kompilieren. Nach dem Import eines Migrationspaketes oder eines kompletten Kundenkonfigurationspaketes wird die Kompilierung der Datenbank aus dem Configuration Wizard oder dem Database Transporter heraus sofort gestartet. Nach dem Import von Hotfixpaketen oder eingeschränkten Kundenkonfigurationspaketen sowie nach Änderungen von Prozessen, Skripten, Bildungsvorschriften, Objektdefinitionen, Methodendefinitionen und präprozessorrelevanten Konfigurationsparametern wird der Database Compiler zur Kompilierung der One Identity Manager-Datenbank eingesetzt.
Report Editor	Mit dem Report Editor können Sie Informationen über die One Identity Manager-Objekte in Berichten zusammenzustellen. Sie können diese Daten gruppieren, aggregieren und grafisch darstellen. Bei der Migration werden bereits vordefinierte Berichte mitgeliefert. Mit dem Report Editor können Sie aber auch eigene Berichte erstellen.
Schema Extension	Schema Extension wird zur Erweiterung des One Identity Manager Schemas um kundenspezifische Tabellen und Spalten eingesetzt. Mit der im One Identity Manager verwendeten Objekttechnologie ist es möglich, das Anwendungsdatenmodell kundenspezifisch um Spalten und Tabellen auf Datenbankebene zu erweitern, sodass diese Erweiterungen auf der Objektebene mit allen Funktionen verfügbar sind.
System Debugger	Mit dem System Debugger können Sie Skripte

Werkzeug	Kurzbeschreibung
	bearbeiten und testen. Die in Ihrer One Identity Manager-Datenbank vorhandenen Skripte werden in eine Visual Studio Skriptbibliothek importiert. Dort können Sie die Skripte lokal bearbeiten und testen. Anschließend entscheiden Sie, ob Ihre Änderungen in die One Identity Manager-Datenbank übernommen werden sollen.
Database Transporter	Der Database Transporter wird eingesetzt, um Objekte und kundenspezifische Anpassungen sowie kundenspezifische Datenbankprozeduren, Trigger, Funktionen und Views aus einer One Identity Manager-Datenbank (Quellsystem) in eine andere One Identity Manager-Datenbank (Zielsystem) zu transportieren.
Job Service Configuration	Job Service Configuration ist das Werkzeug mit dem die Konfigurationsdatei für den One Identity Manager Service erstellt und angepasst wird. Mit dieser Datei werden der One Identity Manager Service selbst und seine Plugins konfiguriert. Die Konfigurationsdatei ist sowohl für den One Identity Manager Service auf einem Windows Betriebssystem als auch für den Linux-Deamon notwendig.
License Meter	Mit dem License Meter führen Sie eine Lizenzvermessung Ihrer One Identity Manager-Datenbank durch. Der Assistent erstellt einen Bericht mit den Lizenz-relevanten Informationen.
Software Loader	Mit dem Software Loader werden neue oder geänderte Dateien, beispielsweise kundenspezifische Formulararchive, in die One Identity Manager-Datenbank geladen um diese über die Mechanismen der automatischen Softwareaktualisierung an die Arbeitsstationen und Jobserver eines One Identity Manager-Netzwerkes zu verteilen.
Server Installer	Mit dem Server Installer können Sie den One Identity Manager Service installieren und konfigurieren. Mit dem Server Installer können Sie den One Identity Manager Service lokal oder remote installieren.
API Server	Der API Server stellt eine API zur Verfügung. Zudem stellt er das Web Portal, das Kennwort-rücksetzungsportal sowie das Web Portal für Betriebs-unterstützung und Ihre HTML-Webanwendungen zur Verfügung.

Verwandte Themen

- Welche Komponenten und Frontends arbeiten mit einem Anwendungsserver? auf Seite 20

Welche Komponenten und Frontends arbeiten mit einem Anwendungsserver?

Der nachfolgenden Liste entnehmen Sie, welche der Komponenten des One Identity Manager gegen einen Anwendungsserver arbeiten können. Einige Frontends arbeiten nur mit eingeschränkter Funktionalität gegen einen Anwendungsserver.

Tabelle 2: One Identity Manager Komponenten und Anwendungsserver

Komponente	Verbindung über Anwendungsserver möglich?	Einschränkungen
Launchpad	Ja	Einige der Anwendungen, die aus dem Launchpad gestartet werden, benötigen eine direkte Verbindung zur Datenbank.
Web Portal	Ja	
Kennwortrücksetzungsportal	Ja	
Web Portal für Betriebsunterstützung	Ja	
Manager	Ja	Die Konsistenzprüfung wird nicht unterstützt. Die Simulation der Complianceregeln wird nicht unterstützt. Einige Formulare werden nicht unterstützt.
Manager Webanwendung	Ja	Einige Formulare werden nicht unterstützt.
Synchronization Editor	Ja	
Analyzer	Ja	
Job Queue Info	Nein	
Configuration Wizard	Nein	
Designer	Ja	Die Konsistenzprüfung wird

Komponente	Verbindung über Anwendungsserver möglich?	Einschränkungen
		nicht unterstützt. Die Simulation von Prozessen wird nicht unterstützt. Das Kompilieren der Datenbank wird nicht unterstützt.
Web Designer	Ja	
Data Import	Ja	
Crypto Configuration	Nein	
Database Compiler	Nein	
Report Editor	Ja	Testen von SQL Abfragen wird nicht unterstützt.
Schema Extension	Nein	
System Debugger	Nein	
Database Transporter	Nein	
License Meter	Ja	
Software Loader	Ja	
One Identity Manager Service	Ja	
Server Installer	Ja	
API Server	Ja	
Database Agent Service	Nein	

3

Installationsvoraussetzungen

Die nachfolgend beschriebenen Installationsvoraussetzungen stellen lediglich Mindestanforderungen zur Inbetriebnahme und uneingeschränkten Nutzung des One Identity Manager dar. Abhängig von der Projektgröße und den unterstützten Geschäftsprozessen und Geschäftsvorfällen können diese Voraussetzungen als Ansatzpunkt für weitere Planungen verwendet werden. Die Ermittlung und gegebenenfalls Weiterentwicklung von Hardwarekapazitäten ist Bestandteil der Projektplanung und abhängig von der Spezifikation des Identity Management Projektes. Besonderes Augenmerk muss auf I/O Performance (in Durchsatz und Latenz) gelegt werden, insbesondere in SAN Umgebungen empfiehlt sich eine gezielte Leistungsanalyse der konkreten Infrastruktur vor dem Einsatz.

Jede One Identity Manager Installation kann virtualisiert werden. Stellen Sie sicher, dass der jeweiligen One Identity Manager-Komponente die laut Systemanforderung spezifizierte Leistung und Ressourcen zur Verfügung stehen. Idealerweise sollten Ressourcenzuordnungen für den Datenbankserver statisch festgesetzt werden. Die Virtualisierung einer One Identity Manager Installation sollte von Experten mit einem fundierten Wissen über Virtualisierungstechniken vorgenommen werden. Weitere Informationen zur Umgebungsvirtualisierung finden Sie in den Richtlinien für den Produkt-Support.

HINWEIS: Sollten für den Einsatz einzelner One Identity Manager Module zusätzliche Systemanforderungen und Berechtigungen erforderlich sein, so werden diese in den entsprechenden Handbüchern aufgeführt.

Detaillierte Informationen zum Thema

- Unterstützte Datenbanksysteme auf Seite 23
- Minimale Systemanforderungen für den Einsatz von SQL Server als Datenbankserver auf Seite 23
- Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank auf Seite 33
- Minimale Systemanforderungen für administrative Arbeitsstationen auf Seite 40
- Minimale Systemanforderungen für Jobserver auf Seite 41
- Minimale Systemanforderungen für den Webserver auf Seite 42
- Minimale Systemanforderungen für den Anwendungsserver auf Seite 44
- Benutzer für den One Identity Manager auf Seite 46

- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29
- Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36
- Einrichten der Berechtigung zum Erstellen eines HTTP Server auf Seite 48
- Kommunikationsports und Firewall Konfiguration auf Seite 48

Unterstützte Datenbanksysteme

One Identity Manager unterstützt folgende Datenbanksysteme:

- SQL Server
- Verwaltete Instanzen in Azure SQL-Datenbank
- Azure SQL-Datenbank

Detaillierte Informationen zum Thema

- Minimale Systemanforderungen für den Einsatz von SQL Server als Datenbankserver auf Seite 23
- Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank auf Seite 33

Minimale Systemanforderungen für den Einsatz von SQL Server als Datenbankserver

Für die Installation einer One Identity Manager-Datenbank sind auf einem Server folgende Systemvoraussetzungen zu gewährleisten. Abhängig von der Anzahl der One Identity Manager Module und der verwalteten Konten im One Identity Manager kann der Bedarf an Arbeitsspeicher, Festplattenspeicher und Prozessoren deutlich über den Minimalanforderungen liegen.

Tabelle 3: Minimale Systemanforderungen - Datenbankserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung (nicht-produktiv) 16 physische Kerne mit 2.5 GHz+ Taktung (produktiv) HINWEIS: Aus Performancegründen wird der Einsatz von 16 physischen Kernen empfohlen.
Arbeitsspeicher	16 GB+ RAM (nicht-produktiv)

	64 GB+ RAM (produktiv)
Freier Festplattenspeicher	100 GB
Betriebssystem	Windows Betriebssysteme • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. UNIX und Linux Betriebssysteme • Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.
Software	Unterstützt werden die Versionen: • SQL Server 2019 Standard Edition (64-Bit) mit aktuellem kumulativen Update • SQL Server 2022 Standard Edition (64-Bit) mit aktuellem kumulativen Update HINWEIS: Aus Performancegründen wird für produktive Systeme der Einsatz der SQL Server Enterprise Edition empfohlen. • SQL Server Management Studio (empfohlen)

HINWEIS: Die zuvor aufgeführten minimalen Systemanforderungen sind für die allgemeine Verwendung gedacht. Bei jeder kundendefinierten One Identity Manager-Bereitstellung müssen diese Werte möglicherweise erhöht werden, um eine ideale Leistung zu erzielen. Um die Anforderungen an die produktive Hardware zu ermitteln, wird dringend empfohlen, einen qualifizierten One Identity-Partner oder das One Identity Professional Services-Team zu konsultieren. Andernfalls kann es zu einer schlechten Datenbankleistung kommen.

Für zusätzliche Hardwareempfehlungen lesen Sie den KB-Artikel https://-support.oneidentity.com/identity-manager/kb/290330/how-to-configure-settings-as-per-the-system-information-overview, in dem die im One Identity Manager verfügbare Übersicht über die Systeminformationen beschrieben wird.

HINWEIS: In virtuellen Umgebungen muss gesichert sein, dass der VM-Host dem Datenbankserver die laut Systemanforderung spezifizierte Leistung und Ressourcen zur Verfügung stellt. Idealerweise sollten Ressourcenzuordnungen für den Datenbankserver statisch festgesetzt werden. Des Weiteren ist eine optimale I/O Performance insbesondere für den Datenbankserver zwingend erforderlich. Weitere Informationen zur Umgebungsvirtualisierung finden Sie in den Richtlinien für den Produkt-Support.

Verwandte Themen

- Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank auf einem SQL Server auf Seite 25

- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29

Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank auf einem SQL Server

Für die Installation und den Betrieb einer One Identity Manager-Datenbank werden folgende Einstellungen des Datenbankservers und der Datenbank vorausgesetzt.

Tabelle 4: Einstellungen für den Datenbankserver

Eigenschaft	Wert	Anmerkung
Sprache (Language)	English	Als Standardsprache für Datenbankbenutzer ist ebenfalls **English** auszuwählen.
Serversortierung (Server Collation)	Case-Insensitiv SQL_Latin1_ General_CP1_CI_AS (empfohlen)	
Extreme Transaktionsverarbeitung unterstützt (Is XTP Supported)	True	One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe. Der Datenbankserver muss die extreme Transaktionsverarbeitung (XTP) unterstützen. In einer Standardinstallation ist diese Funktion aktiviert. Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft. Ist XTP nicht aktiviert, wird die Installation oder Aktualisierung nicht gestartet.

Tabelle 5: Einstellungen für die Datenbank

Eigenschaft	Wert	Anmerkung
Sortierung (Collation)	SQL_Latin1_ General_CP1_CI_	Die Einstellung wird durch den Configuration Wizard vor einer Installation

Eigenschaft	Wert	Anmerkung
	AS	oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Wiederherstellungsmodell (Recovery model)	Einfach (Simple)	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft. Ist das Wiederherstellungsmodell nicht auf den Wert **Einfach** gesetzt, wird vor der Installation oder Aktualisierung eine Warnung ausgegeben. Diese Warnung kann ignoriert werden. Aus Performancegründen wird jedoch empfohlen, für die Zeit der Schemainstallation oder der Schemaaktualisierung die Datenbank auf das Wiederherstellungsmodell **Einfach** zu setzen.
Kompatibilitätsgrad (Compatibility level)	SQL Server 2019 (150)	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Statistiken automatisch erstellen (Auto Create Statistics)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Statistiken automatisch aktualisieren (Auto Update Statistics)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Statistiken automatisch asynchron aktualisieren (Auto Update Statistics Asynchronously)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank

Eigenschaft	Wert	Anmerkung
		eingestellt.
Abbruch bei arithmetischem Fehler aktiviert (Arithmetic Abort enabled)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Bezeichner in Anführungszeichen aktiviert (Quoted Identifiers Enabled)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Ist aktivierte READ COMMITTED-Momentaufnahme (Is Read Committed Snapshot On)	True	Die Standardeinstellung für Transaktionen ist **AutoCommit**. Werden Transaktionen benötigt, werden diese explizit eröffnet. Diese Einstellungen haben sich als beste Abwägung von Datensicherheit und Performance innerhalb der massiven Parallelverarbeitung für One Identity Manager herausgestellt. Andere Transaktionsmodi werden vom One Identity Manager nicht unterstützt. Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Parametrisierung (Parameterization)	Forced	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Datenbankdatei und Datendateigruppe für speicheroptimierte Tabellen	Erforderlich	One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe.

Eigenschaft	Wert	Anmerkung
		Für die Erstellung speicheroptimierter Tabellen sind folgende Voraussetzungen zu erfüllen: • Es muss eine Datenbankdatei mit den Dateityp **Filestream-Daten** (Filestream data) vorhanden sein. • Es muss eine speicheroptimierte Datendateigruppe (Memory-optimized data filegroup) vorhanden sein. Vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft der Configuration Wizard, ob diese Anforderungen erfüllt sind. Es werden im Configuration Wizard Reparaturmethoden angeboten, um die Datenbankdatei und die Datendateigruppe zu erstellen. Die Datenbankdatei wird durch die Reparaturmethode im Verzeichnis der Datendatei (`*.mdf`) erstellt.
Verzögerte Kompilierung von Tabellenvariablen (Table variable deferred compilation) (DEFERRED_COMPILATION_TV)	ON	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Verschachtelte Ausführung (Interleaved Execution) (INTERLEAVED_EXECUTION_TVF)	ON	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.

Ausführliche Informationen zu den genannten Datenbankservereigenschaften finden Sie unter https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/view-or-change-server-properties-sql-server.

Ausführliche Informationen zu den genannten Datenbankeigenschaften finden Sie unter https://docs.microsoft.com/en-us/sql/relational-databases/databases/view-or-change-the-properties-of-a-database und https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-databases-transact-sql.

Verwandte Themen

- Minimale Systemanforderungen für den Einsatz von SQL Server als Datenbankserver auf Seite 23
- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29
- Fehlermeldungen bei der Installation und der Aktualisierung der One Identity Manager-Datenbank auf Seite 190

Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server

Für den Einsatz einer One Identity Manager-Datenbank auf einem SQL Server mit dem abgestufte Berechtigungskonzept werden folgende Benutzer unterschieden. Die Berechtigungen der Benutzer auf Serverebene und Datenbankebene sind auf ihre Aufgaben abgestimmt.

HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

- Installationsbenutzer

  Der Installationsbenutzer wird für die initiale Installation einer One Identity Manager-Datenbank mit dem Configuration Wizard benötigt.

  HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 9.1.3 auf das abgestufte Berechtigungskonzept wechseln möchten, benötigen Sie ebenfalls diesen Installationsbenutzer.

- Administrativer Benutzer

  Der administrative Benutzer wird durch Komponenten des One Identity Manager verwendet, die Berechtigungen auf Serverebene und Datenbankebene benötigen, beispielsweise der Configuration Wizard, der DBQueue Prozessor oder der One Identity Manager Service.

- Konfigurationsbenutzer

  Der Konfigurationsbenutzer kann Konfigurationsaufgaben innerhalb des One Identity Manager ausführen, beispielsweise kundenspezifischen Schemaerweiterungen erstellen oder mit dem Designer arbeiten. Konfigurationsbenutzer benötigen Berechtigungen auf Serverebene und Datenbankebene.

- Endbenutzer

  Endbenutzer erhalten nur Berechtigungen auf Datenbankebene, um beispielsweise Aufgaben mit dem Manager oder dem Web Portal zu erfüllen.

Ausführliche Informationen zu den minimalen Berechtigungsebenen der One Identity Manager-Werkzeuge finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Berechtigungen für den Installationsbenutzer

Für den Installationsbenutzer müssen eine SQL Server Anmeldung und ein Datenbankbenutzer mit den folgenden Berechtigungen zur Verfügung gestellt werden.

SQL Server:

- Mitglied der Serverrolle **dbcreator**

  Die Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird.

- Mitglied der Serverrolle **sysadmin**

  Diese Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird und dabei die Verzeichnisse für die Dateien über den Dateibrowser gewählt werden müssen. Werden die Dateien in den Standardverzeichnissen des Datenbankservers abgelegt, wird die Berechtigung nicht benötigt.

- Mitglied der Serverrolle **securityadmin**

  Diese Serverrolle wird für die Erstellung der SQL Server Anmeldungen benötigt.

- Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

  Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

- Berechtigung **alter any server role**

  Die Berechtigung wird benötigt, um die Serverrolle für den administrativen Benutzer zu erzeugen.

msdb-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

master-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

- Berechtigung **Execute** mit der Option **with grant option** für die Prozedur `xp_readerrorlog`

  Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.

One Identity Manager-Datenbank:

- Mitglied der Datenbankrolle **db_owner**

  Diese Datenbankrolle wird benötigt, wenn bei der Installation des Schemas mit dem Configuration Wizard eine vorhandene Datenbank verwendet werden soll oder eine Aktualisierung des Schemas erfolgt.

Berechtigungen für den administrativen Benutzer

Für den administrativen Benutzer werden während der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **alter any server role**

    Die Berechtigung wird benötigt, um die Serverrolle für den Konfigurationsbenutzer zu erzeugen.
  - Berechtigung **view any definition**

    Die Berechtigung wird benötigt, um die SQL Server Anmeldungen für den Konfigurationsbenutzer und den Endbenutzer mit den entsprechenden Datenbankbenutzern zu verbinden.
- SQL Server Anmeldung **<DatabaseName>_Admin**
  - Mitglied der Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

    Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

master-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
  - Berechtigung **Execute** für die Prozedur `xp_readerrorlog`

    Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.

- Datenbankbenutzer **OneIM_<DatabaseName>**
  - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

One Identity Manager-Datenbank:

- Datenbankbenutzer **Admin**
  - Mitglied in Datenbankrolle **db_owner**

    Die Datenbankrolle wird benötigt, um eine Datenbank mit dem Configuration Wizard zu aktualisieren.
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

Berechtigungen für den Konfigurationsbenutzer

Für Konfigurationsbenutzer werden während der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMConfigRole_<DatabaseName>**
  - Berechtigung **view server state** und Berechtigung **alter any connection**

    Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.
- SQL Anmeldung **<DatabaseName>_Config**
  - Mitglied der Serverrolle **OneIMConfigRole_<DatabaseName>**

One Identity Manager-Datenbank:

- Datenbankrolle **OneIMConfigRoleDB**
  - Berechtigungen **Create procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create view**, **Insert**, **Execute**, **Create function** auf die Datenbank
- Datenbankbenutzer **Config**
  - Mitglied der Datenbankrolle **OneIMConfigRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_Config** verbunden.

Berechtigungen für den Endbenutzer

Für Endbenutzer werden während der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- SQL Anmeldung **<DatabaseName>_User**

One Identity Manager-Datenbank:

- Datenbankrolle **OneIMUserRoleDB**
  - Berechtigungen **Insert**, **Update**, **Select**, **Delete** auf ausgewählte Tabellen der Datenbank
  - Berechtigung **view definition** auf die Datenbank
  - Berechtigungen **Execute** und **References** für einzelne Funktionen, Prozeduren und Typen
- Datenbankbenutzer **User**
  - Mitglied der Datenbankrolle **OneIMUserRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_User** verbunden.

Hinweise zur Nutzung der integrierten Windows Authentifizierung

Die integrierte Windows Authentifizierung kann für den One Identity Manager Service und die Webanwendungen uneingeschränkt genutzt werden. Für die Fat-Clients kann die integrierte Windows Authentifizierung genutzt werden. Die Nutzung von Windows Gruppen zur Anmeldung wird unterstützt. Zur Sicherstellung der Funktionalität wird jedoch dringend die Nutzung einer SQL Server Anmeldung empfohlen.

Um die integrierte Windows Authentifizierung einzusetzen

- Richten Sie für das Benutzerkonto auf dem Datenbankserver eine SQL Server Anmeldung ein.
- Tragen Sie als Standardschema **dbo** ein.
- Weisen Sie der SQL Server Anmeldung die benötigten Berechtigungen zu.

Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank

Um die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank zu betreiben, wird der Tarif **Unternehmenskritisch** benötigt. Ausführliche Informationen finden Sie bei Microsoft unter https://azure.microsoft.com/en-us/services/sql-database/.

Verwandte Themen

- Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 34
- Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36

Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank

Für die Installation und den Betrieb einer One Identity Manager-Datenbank werden folgende Einstellungen des Datenbankservers und der Datenbank vorausgesetzt.

Tabelle 6: Einstellungen für den Datenbankserver

Eigenschaft	Wert	Anmerkung
Sprache (Language)	English	Als Standardsprache für Datenbankbenutzer ist ebenfalls **English** auszuwählen.
Serversortierung (Server Collation)	Case-Insensitiv SQL_Latin1_General_CP1_CI_AS (empfohlen)	
Extreme Transaktionsverarbeitung unterstützt (Is XTP Supported)	True	Standardeinstellung.

Tabelle 7: Einstellungen für die Datenbank

Eigenschaft	Wert	Anmerkung
Sortierung (Collation)	SQL_Latin1_General_CP1_CI_AS	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Wiederherstellungsmodell (Recovery model)	Vollständig (Full)	Standardeinstellung.

Eigenschaft	Wert	Anmerkung
Kompatibilitätsgrad (Compatibility level)	SQL Server 2019 (150)	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Statistiken automatisch erstellen (Auto Create Statistics)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Statistiken automatisch aktualisieren (Auto Update Statistics)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Statistiken automatisch asynchron aktualisieren (Auto Update Statistics Asynchronously)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Abbruch bei arithmetischem Fehler aktiviert (Arithmetic Abort enabled)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Bezeichner in Anführungszeichen aktiviert (Quoted Identifiers Enabled)	True	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Ist aktivierte READ COMMITTED-Momentaufnahme (Is Read Committed Snapshot On)	True	Die Standardeinstellung für Transaktionen ist **AutoCommit**. Werden Transaktionen benötigt, werden diese explizit eröffnet. Diese Einstellungen haben sich als

Eigenschaft	Wert	Anmerkung
		beste Abwägung von Datensicherheit und Performance innerhalb der massiven Parallelverarbeitung für One Identity Manager herausgestellt. Andere Transaktionsmodi werden vom One Identity Manager nicht unterstützt. Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Parametrisierung (Parameterization)	Forced	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Datenbankdatei und Datendateigruppe für speicheroptimierte Tabellen	Erforderlich	Standardeinstellung.
Verzögerte Kompilierung von Tabellenvariablen (Table variable deferred compilation) (DEFERRED_COMPILATION_TV)	ON	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.
Verschachtelte Ausführung (Interleaved Execution) (INTERLEAVED_EXECUTION_TVF)	ON	Die Einstellung wird durch den Configuration Wizard vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank geprüft und gegebenenfalls für die Datenbank eingestellt.

Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank

Für den Einsatz einer One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank mit dem abgestufte Berechtigungskonzept werden folgende

Benutzer unterschieden. Die Berechtigungen der Benutzer auf Serverebene und Datenbankebene sind auf ihre Aufgaben abgestimmt.

- Installationsbenutzer

  Der Installationsbenutzer wird für die initiale Installation einer One Identity Manager-Datenbank mit dem Configuration Wizard benötigt.

- Administrativer Benutzer

  Der administrative Benutzer wird durch Komponenten des One Identity Manager verwendet, die Berechtigungen auf Serverebene und Datenbankebene benötigen, beispielsweise der Configuration Wizard, der DBQueue Prozessor oder der One Identity Manager Service.

- Konfigurationsbenutzer

  Der Konfigurationsbenutzer kann Konfigurationsaufgaben innerhalb des One Identity Manager ausführen, beispielsweise kundenspezifischen Schemaerweiterungen erstellen oder mit dem Designer arbeiten. Konfigurationsbenutzer benötigen Berechtigungen auf Serverebene und Datenbankebene.

- Endbenutzer

  Endbenutzer erhalten nur Berechtigungen auf Datenbankebene, um beispielsweise Aufgaben mit dem Manager oder dem Web Portal zu erfüllen.

Ausführliche Informationen zu den minimalen Berechtigungsebenen der One Identity Manager-Werkzeuge finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Berechtigungen für den Installationsbenutzer

Für den Installationsbenutzer müssen eine SQL Server Anmeldung und ein Datenbankbenutzer mit den folgenden Berechtigungen zur Verfügung gestellt werden.

SQL Server:

- Mitglied der Serverrolle **dbcreator**

  Die Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird.

- Mitglied der Serverrolle **securityadmin**

  Diese Serverrolle wird für die Erstellung der SQL Server Anmeldungen benötigt.

- Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

  Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

- Berechtigung **alter any server role**

  Die Berechtigung wird benötigt, um die Serverrolle für den administrativen Benutzer zu erzeugen.

msdb-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

master-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

- Berechtigung **Execute** mit der Option **with grant option** für die Prozedur `xp_readerrorlog`

  Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.

One Identity Manager-Datenbank:

- Mitglied der Datenbankrolle **db_owner**

  Diese Datenbankrolle wird benötigt, wenn bei der Installation des Schemas mit dem Configuration Wizard eine vorhandene Datenbank verwendet werden soll oder eine Aktualisierung des Schemas erfolgt.

Berechtigungen für den administrativen Benutzer

Für den administrativen Benutzer werden während der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **alter any server role**

    Die Berechtigung wird benötigt, um die Serverrolle für den Konfigurationsbenutzer zu erzeugen.

  - Berechtigung **view any definition**

    Die Berechtigung wird benötigt, um die SQL Server Anmeldungen für den Konfigurationsbenutzer und den Endbenutzer mit den entsprechenden Datenbankbenutzern zu verbinden.

- SQL Server Anmeldung **<DatabaseName>_Admin**

        - Mitglied der Serverrolle **OneIMAdminRole_<DatabaseName>**
        - Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

          Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

master-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
    - Berechtigung **Execute** für die Prozedur `xp_readerrorlog`

      Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.
- Datenbankbenutzer **OneIM_<DatabaseName>**
    - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
    - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

One Identity Manager-Datenbank:

- Datenbankbenutzer **Admin**
    - Mitglied in Datenbankrolle **db_owner**

      Die Datenbankrolle wird benötigt, um eine Datenbank mit dem Configuration Wizard zu aktualisieren.
    - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

Berechtigungen für den Konfigurationsbenutzer

Für Konfigurationsbenutzer werden während der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMConfigRole_<DatabaseName>**
    - Berechtigung **view server state** und Berechtigung **alter any connection**

      Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.
- SQL Anmeldung **<DatabaseName>_Config**
    - Mitglied der Serverrolle **OneIMConfigRole_<DatabaseName>**

One Identity Manager-Datenbank:

- Datenbankrolle **OneIMConfigRoleDB**
  - Berechtigungen **Create procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create view**, **Insert**, **Execute**, **Create function** auf die Datenbank
- Datenbankbenutzer **Config**
  - Mitglied der Datenbankrolle **OneIMConfigRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_Config** verbunden.

Berechtigungen für den Endbenutzer

Für Endbenutzer werden während der Installation der One Identity Manager-Datenbank mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- SQL Anmeldung **<DatabaseName>_User**

One Identity Manager-Datenbank:

- Datenbankrolle **OneIMUserRoleDB**
  - Berechtigungen **Insert**, **Update**, **Select**, **Delete** auf ausgewählte Tabellen der Datenbank
  - Berechtigung **view definition** auf die Datenbank
  - Berechtigungen **Execute** und **References** für einzelne Funktionen, Prozeduren und Typen
- Datenbankbenutzer **User**
  - Mitglied der Datenbankrolle **OneIMUserRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_User** verbunden.

Minimale Systemanforderungen für administrative Arbeitsstationen

Zur Darstellung und Bearbeitung von Daten werden die Administrationswerkzeuge und Konfigurationswerkzeuge des One Identity Manager auf einer administrativen Arbeitsstation installiert.

Zur Installation der One Identity Manager-Komponenten auf einer administrativen Arbeitsstation sind die folgenden Systemvoraussetzungen zu gewährleisten.

Tabelle 8: Minimale Systemanforderungen - Administrative Arbeitsstation

Prozessor	4 physische Kerne mit 2 GHz+ Taktung
Arbeitsspeicher	4 GB+ RAM
Freier Festplattenspeicher	1 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows 11 (x64) • Windows 10 (32-Bit oder 64-Bit) mindestens Version 1511 • Windows 8.1 (32-Bit oder 64-Bit) mit dem aktuellen Service Pack
Zusätzliche Software	• Microsoft .NET Framework Version 4.8 oder höher • Microsoft Edge WebView2
Unterstützte Browserversionen	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimale Systemanforderungen für Jobserver

Der One Identity Manager Service sorgt für die Verbreitung der in der One Identity Manager-Datenbank verwalteten Informationen im Netzwerk. Der One Identity Manager Service übernimmt die Datensynchronisation zwischen Datenbank und den angebundenen Zielsystemen sowie die Durchführung von Aktionen auf Datenbank- und Dateiebene.

Der One Identity Manager Service wird auf einem Server installiert. Ein Server, auf dem der One Identity Manager Service installiert ist, wird nachfolgend als Jobserver bezeichnet.

Zur Installation des One Identity Manager Service sind auf einem Server folgende Systemvoraussetzungen zu gewährleisten.

Tabelle 9: Minimale Systemanforderungen - Jobserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	16 GB RAM
Freier Festplattenspeicher	40 GB

Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden.
Zusätzliche Software	Windows Betriebssysteme • Microsoft .NET Framework Version 4.8 oder höher HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers. Linux Betriebssysteme • Mono 6.10 oder höher HINWEIS: Es kann notwendig sein, die Umgebungsvariable `MONO_PATH` explizit auf das aktuelle Installationsverzeichnis zu setzen, um sicherzustellen, dass alle referenzierten Assemblies geladen werden können.

Verwandte Themen

- Benutzer für den One Identity Manager auf Seite 46

Minimale Systemanforderungen für den Webserver

Zur Installation der Webanwendungen sind auf einem Webserver folgende Systemvoraussetzungen zu gewährleisten.

Tabelle 10: Systemanforderungen - Webserver

Prozessor	4 physische Kerne mit 1.65 GHz+Taktung
Arbeitsspeicher	4 GB RAM

Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden. Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für Apache HTTP Server.

Zusätzliche Software	Windows Betriebssysteme
	• Microsoft .NET Framework Version 4.8 oder höher
	• Microsoft Internet Information Services 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.8 und den Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions
	  • Web Server > Application Development > ISAPI Filters
	  • Web Server > Security > Basic Authentication
	  • Web Server > Security > Windows Authentication
	  • Web Server > Performance > Static Content Compression
	  • Web Server > Performance > Dynamic Content Compression

	Linux Betriebssysteme
	• NTP - Client
	• Mono 6.10 oder höher
	• Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
	  • mod_mono
	  • rewrite
	  • ssl (optional)

Minimale Systemanforderungen für den Anwendungsserver

Der Anwendungsserver stellt einen Verbindungspool für den Zugriff auf die Datenbank zu Verfügung und hält die Geschäftslogik. Zur Installation des Anwendungsservers sind die folgenden Systemvoraussetzungen zu gewährleisten.

Tabelle 11: Systemanforderungen - Anwendungsserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	8 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden. Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für Apache HTTP Server.
Zusätzliche Software	Windows Betriebssysteme

- Microsoft .NET Framework Version 4.8 oder höher
- Microsoft Internet Information Services 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.8 und den Role Services:
    - Web Server > Common HTTP Features > Static Content
    - Web Server > Common HTTP Features > Default Document
    - Web Server > Application Development > ASP.NET
    - Web Server > Application Development > .NET Extensibility
    - Web Server > Application Development > ISAPI Extensions
    - Web Server > Application Development > ISAPI Filters
    - Web Server > Security > Basic Authentication
    - Web Server > Security > Windows Authentication
    - Web Server > Performance > Static Content Compression
    - Web Server > Performance > Dynamic Content Compression

Linux Betriebssysteme

- NTP - Client
- Mono 6.10 oder höher
- Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
    - mod_mono
    - rewrite
    - ssl (optional)

HINWEIS: Zur Verwendung der REST API des Anwendungsserver müssen die HTTP-Anfragemethoden `POST`, `GET`, `PUT` und `DELETE` vom Webserver (IIS/Apache) zugelassen werden.

Benutzer für den One Identity Manager

Tabelle 12: Benutzer für den One Identity Manager

Benutzer	Berechtigungen
Benutzer zur Installation des One Identity Manager	Der Installationsbenutzer wird für die initiale Installation einer One Identity Manager-Datenbank mit dem Configuration Wizard benötigt. Ausführliche Informationen finden Sie unter Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29 und Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36.
Benutzer für administrative Aufgaben im One Identity Manager	Der administrative Benutzer wird durch Komponenten des One Identity Manager verwendet, die Berechtigungen auf Serverebene und Datenbankebene benötigen, beispielsweise der Configuration Wizard, der DBQueue Prozessor oder der One Identity Manager Service. Ausführliche Informationen finden Sie unter Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29 und Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36.
Benutzer für Konfigurationsaufgaben im One Identity Manager	Der Konfigurationsbenutzer kann Konfigurationsaufgaben innerhalb des One Identity Manager ausführen, beispielsweise kundenspezifischen Schemaerweiterungen erstellen oder mit dem Designer arbeiten. Konfigurationsbenutzer benötigen Berechtigungen auf Serverebene und Datenbankebene. Ausführliche Informationen finden Sie unter Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29 und Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36.
Endbenutzer für One Identity Manager	Endbenutzer erhalten nur Berechtigungen auf Datenbankebene, um beispielsweise Aufgaben mit dem Manager oder dem Web Portal zu erfüllen. Ausführliche Informationen finden Sie unter Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29 und Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36.
Benutzer zur Anmeldung am One Identity Manager	Zur Anmeldung an den Administrationswerkzeugen verwendet der One Identity Manager unterschiedliche Authen-

Benutzer	Berechtigungen
	tifizierungsmodule. Die Authentifizierungsmodule ermitteln den anzuwendenden Systembenutzer und laden abhängig von dessen Berechtigungsgruppen die Benutzeroberfläche und die Berechtigungen auf Ressourcen der Datenbank. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
Benutzerkonto für den One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen) HINWEIS: Für die Synchronisation des One Identity Manager mit den einzelnen Zielsystemen können weitere zielsystemspezifische Berechtigungen erforderlich sein. Diese Berechtigungen werden in den entsprechenden Handbüchern erläutert. Weitere Informationen finden Sie unter Einrichten der Berechtigung zum Erstellen eines HTTP Server auf Seite 48.

Einrichten der Berechtigung zum Erstellen eines HTTP Server

Die Anzeige der Protokolldateien des One Identity Manager Service kann über einen HTTP Server erfolgen (http://<Servername>:<Portnummer>).

Damit ein Benutzer einen HTTP Server öffnen kann, muss er dazu berechtigt werden. Dazu muss der Administrator dem Benutzer die URL Genehmigung erteilen. Dies kann über folgenden Kommandozeilenaufruf erfolgen:

```
netsh http add urlacl url=http://*:<Portnummer>/ user=<Domäne>\<Benutzername>
```

Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so müssen explizit Berechtigungen für den internen Webservice vergeben werden. Dies kann über folgenden Kommandozeilenaufruf erfolgen:

```
netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT
AUTHORITY\NETWORKSERVICE"
```

Das Ergebnis können Sie gegebenenfalls über folgenden Kommandozeilenaufruf prüfen:

```
netsh http show urlacl
```

Kommunikationsports und Firewall Konfiguration

Der One Identity Manager besteht aus verschiedenen Komponenten, die in verschiedenen Netzwerksegmenten laufen können. Zusätzlich benötigt der One Identity Manager Zugriff auf verschiedene Netzwerkdienste, welche ebenfalls in verschiedenen Netzwerksegmenten installiert sein können. Abhängig davon, welche Komponenten und Dienste Sie hinter ihrer Firewall installieren möchten, müssen Sie verschiedene Ports öffnen.

Die folgenden Basisports werden benötigt.

Tabelle 13: Kommunikationsports

Standardport	Beschreibung
1433	Port zur Kommunikation mit der One Identity Manager-Datenbank.
80	Port für den Zugriff auf die Webanwendungen.
88	Kerberos-Authentifizierungssystem (wenn Kerberos Authentifizierung eingesetzt wird).
135	Microsoft End Point Mapper (EPMAP) (auch DCE/RPC Locator Service).
137	NetBIOS Name Service.

Standardport	Beschreibung
139	NetBIOS Session Service.
443	Standardport für HTTPS-Verbindungen.
1880	Port für das HTTP-basierte Protokoll des One Identity Manager Service.
2880	Port für die Zugriffstests innerhalb des Synchronization Editor, beispielsweise im Zielsystembrowser oder zur Simulation der Synchronisation. Standardport für das `RemoteConnectPlugin`.

Für die Verbindung zu den Zielsystemen können weitere Ports erforderlich sein. Diese Ports werden in den entsprechenden Handbüchern aufgeführt.

4

Installieren des One Identity Manager

Um den One Identity Manager zu installieren, sind folgende Schritte erforderlich:

1. Installieren der One Identity Manager-Komponenten auf der administrativen Arbeitsstation, auf welcher die Schemainstallation der One Identity Manager-Datenbank gestartet wird.
2. Installieren und Konfigurieren des One Identity Manager-Datenbank mit dem Configuration Wizard.
3. Einrichten eines Servers, der die Verarbeitung von SQL Prozessen übernimmt.
   - Der Server muss als Jobserver mit der Serverfunktion **SQL Ausführungsserver** in der Datenbank eingetragen sein.
   - Auf dem Server muss ein One Identity Manager Service mit direktem Zugriff auf die One Identity Manager-Datenbank installiert und konfiguriert sein.

   HINWEIS: Für ein Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden.
4. Einrichten eines Aktualisierungsservers für die automatische Softwareaktualisierung weiterer Server.
   - Der Server muss als Jobserver mit der Serverfunktion **Aktualisierungsserver** in der Datenbank eingetragen sein.
   - Auf dem Server muss ein One Identity Manager Service mit direktem Zugriff auf die One Identity Manager-Datenbank installiert und konfiguriert sein.
5. Einrichten und Konfigurieren des Database Agent Service.

   Der Database Agent Service steuert die Verarbeitung der DBQueue Prozessor Aufträge. Der Database Agent Service wird über ein Plugin des One Identity Manager Service bereitgestellt. Alternativ kann der Database Agent Service über das Kommandozeilenprogramm `DatabaseAgentServiceCmd.exe` ausgeführt werden.

HINWEIS: Mit dem Configuration Wizard können Sie bereits einen SQL Ausführungsserver und den Aktualisierungsserver einrichten. Den Database Agent Service können Sie ebenfalls mit den Configuration Wizard einrichten.

Zusätzlich können folgende Installationen ausgeführt werden.

- Installieren weiterer Arbeitsstationen.
- Installieren weiterer Server mit One Identity Manager Service.
- Installieren eines Anwendungsservers.
- Installieren eines API Servers mit HTML-Webanwendungen.
- Installieren des Web Designer Web Portal auf einem Webserver.
- Installieren des Kennwortrücksetzungsportal auf einem Webserver.

  Ausführliche Informationen zur Installation und Konfiguration des Kennwortrücksetzungsportal finden Sie im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.
- Installieren der Manager Webanwendung auf einem Webserver.

One Identity Manager können Sie auf folgende Arten installieren und aktualisieren.

- Die Erstinstallation der One Identity Manager-Komponenten auf den Arbeitsstationen nehmen Sie mit dem Installationsassistenten vor.
- Zur Installation und Aktualisierung der One Identity Manager-Datenbank nutzen Sie den Configuration Wizard.
- Die Erstinstallation des One Identity Manager Service auf den Servern nehmen Sie mit dem Installationsassistenten oder mit dem Server Installer vor.
- Zur Aktualisierung vorhandener Installationen setzen Sie die automatische Softwareaktualisierung ein.
- Für die manuelle Aktualisierung einzelner Arbeitsstationen und einzelner Server nutzen Sie den Installationsassistenten.

HINWEIS: One Identity stellt verschiedene Docker-Images für eine einfache und standardisierte Installation und Ausführung einzelner One Identity Manager-Komponenten in Docker-Containern zur Verfügung.

Detaillierte Informationen zum Thema

- One Identity Manager Docker-Images auf Seite 52
- Bevor Sie die Installation des One Identity Manager starten auf Seite 53
- One Identity Manager-Komponenten installieren auf Seite 53
- Installieren und Konfigurieren einer One Identity Manager-Datenbank auf Seite 58
- Installieren und Konfigurieren des One Identity Manager Service auf Seite 89
- Anwendungsserver installieren auf Seite 136
- Web Designer Web Portal installieren auf Seite 152
- Installieren und Aktualisieren der Manager Webanwendung auf Seite 171
- Aktualisieren des One Identity Manager auf Seite 110

One Identity Manager Docker-Images

One Identity stellt verschiedene Docker-Images für eine einfache und standardisierte Installation und Ausführung einzelner One Identity Manager-Komponenten in Docker-Containern zur Verfügung. Die One Identity Manager Docker-Images sowie ausführliche Informationen zur Verwendung und Konfiguration der einzelnen Images finden Sie unter https://hub.docker.com/u/oneidentity/. Videos mit zusätzlichen Informationen finden Sie in der Videoserie One Identity Manager Containerization unter www.YouTube.com/OneIdentity. Ausführliche Informationen zu Docker finden Sie unter https://www.docker.com/.

Tabelle 14: Verfügbare One Identity Manager Docker-Images

Docker-Image	Beschreibung
oneidentity/oneim-job	Dieses Image führt eine Instanz eines One Identity Manager Service aus. Es lädt beim Start die notwendigen Dateien für einen bestimmten Jobserver herunter. Das Verhalten kann durch verschlüsselte Werte und Umgebungsvariablen gesteuert werden.
oneidentity/oneim-appserver	Dieses Image führt einen Instanz des One Identity Manager Anwendungsservers aus. Es lädt die notwendigen Dateien beim Start aus der konfigurierten One Identity Manager-Datenbank herunter. Das Verhalten kann durch verschlüsselte Werte und Umgebungsvariablen gesteuert werden.
oneidentity/oneim-web	Dieses Image führt eine Instanz des Web Designer Web Portals aus. Es lädt die notwendigen Dateien beim Start aus der konfigurierten One Identity Manager-Datenbank herunter. Das Verhalten kann durch verschlüsselte Werte und Umgebungsvariablen gesteuert werden.
oneidentity/oneim-installer	Dieses Image enthält ein einfaches Installationsprogramm, das in abgeleiteten Images verwendet werden kann, um die Dateistruktur für One Identity Manager Anwendungen zu erstellen.
oneidentity/oneim-api	Dieses Image führt eine Instanz der API Servers aus. Es lädt die notwendigen Dateien beim Start aus der konfigurierten One Identity Manager-Datenbank herunter. Das Verhalten kann durch verschlüsselte Werte und Umgebungsvariablen gesteuert werden.

Unter https://github.com/OneIdentity werden im Docker Files Repository zusätzliche Beispiele für Dockerfiles bereitgestellt. Diese Beispiel können Sie verwenden, um eigene Docker-Container-Images auf Basis der One Identity Manager Docker-Images zu erstellen.

Bevor Sie die Installation des One Identity Manager starten

Bevor Sie die Installation des One Identity Manager starten:

- Stellen Sie sicher, dass die minimalen Hardwarevoraussetzungen und die minimalen Softwarevoraussetzungen auf den Arbeitsstationen und den Servern gewährleistet sind.
- Beenden Sie alle Programmkomponenten und Dienstkomponenten, da sonst die Installation nicht beginnen kann.

Detaillierte Informationen zum Thema

- Installationsvoraussetzungen auf Seite 22
- Installieren des One Identity Manager auf Seite 50
- Aktualisieren des One Identity Manager auf Seite 110

One Identity Manager-Komponenten installieren

Bei der Installation der One Identity Manager-Komponenten auf Arbeitsstationen und Servern werden Sie durch einen Installationsassistenten unterstützt.

HINWEIS: Starten Sie die Installation der Administrationswerkzeuge und Konfigurationswerkzeuge nach Möglichkeit immer auf einer administrativen Arbeitsstation.

HINWEIS: Auf Linux Betriebssystemen wird die Verwendung des Docker-Images oneidentity/oneim-installer empfohlen.

Um die One Identity Manager-Komponenten zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Wechseln Sie auf den Tabreiter **Installation** und wählen Sie die Edition.
3. Klicken Sie **Installieren**.

   Der Installationsassistent wird gestartet.
4. Auf der Startseite wählen Sie die Sprache für den Installationsassistenten und klicken Sie **Weiter**.
5. Bestätigen Sie die Lizenzbedingungen.

6. Auf der Seite **Einstellungen für die Installation** erfassen Sie folgenden Informationen.
    - **Installationsquelle**: Wählen Sie das Verzeichnis mit den Installationsdateien.
    - **Installationsverzeichnis**: Wählen Sie das Verzeichnis, in das die Dateien des One Identity Manager installiert werden sollen.

      HINWEIS: Um weitere Konfigurationseinstellungen vorzunehmen, klicken Sie auf die Pfeil Schaltfläche neben dem Eingabefeld. Hier können Sie festlegen, ob die Installation auf einem 64 Bit- Betriebssystem oder auf einem 32 Bit-Betriebssystem erfolgt.

      Für eine Standardinstallation nehmen Sie keine weiteren Konfigurationseinstellungen vor.
    - **Installationsmodule mit der Datenbank auswählen**: Um die Installationsinformationen über die vorhandene One Identity Manager-Datenbank zu laden sind, aktivieren Sie die Option.

      HINWEIS: Für Installation der Arbeitsstation, auf der Sie die Installation des One Identity Manager Schemas starten, lassen Sie die Option deaktiviert.
    - **Weitere Module zur gewählten Edition hinzufügen**: Um zusätzliche One Identity Manager Module zur gewählten Edition hinzuzufügen, aktivieren Sie die Option.
7. Auf der Seite **Datenbank verbinden** erfassen Sie die Informationen zur Datenbankverbindung.

   HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen** aktiviert haben.
    - Wählen Sie im Bereich **Datenbankverbindung auswählen** die Verbindung.

      - ODER -
    - Klicken Sie auf **Neue Verbindung erstellen**, wählen Sie den Systemtyp **SQL Server** und erfassen Sie die Verbindungsdaten.
        - **Server**: Datenbankserver.
        - (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
        - **Nutzer**: SQL Server Anmeldename des Benutzer.
        - **Kennwort**: Kennwort für die SQL Server Anmeldung des Benutzer.
        - **Datenbank**: Wählen Sie die Datenbank.
8. Auf der Seite **Modulauswahl** wählen Sie die zusätzlich zu installierenden Module.

   HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Option **Weitere Module zur gewählten Edition hinzufügen** aktiviert haben.

9. Auf der Seite **Maschinenrolle zuordnen** legen Sie die Maschinenrollen fest.

   HINWEIS: Bei Auswahl einer Maschinenrolle werden alle untergeordneten Maschinenrollen mit ausgewählt. Sie können einzelne Maschinenrollen abwählen.

   Die folgenden Maschinenrollen können Sie wählen.

   - **Workstation**: Enthält alle Basiskomponenten zur Installation der Werkzeuge auf einer administrativen Arbeitsstation.
   - **Workstation |Administration**: Enthält die Administrationswerkzeuge, die ein Standardbenutzer zur Erfüllung seiner Aufgaben mit dem One Identity Manager benötigt. Neben den Werkzeugen, welche die Grundfunktionalität für die Arbeit mit One Identity Manager sicherstellen, zählt dazu auch der Manager als zentrales Administrationswerkzeug.
   - **Workstation | Configuration**: Enthält alle Werkzeuge des Standardbenutzers und zusätzliche Programme, welche zur Konfiguration des Systems erforderlich sind. Dazu gehören beispielsweise Configuration Wizard,Database Compiler, Database Transporter, Designer sowie Konfigurationswerkzeuge für den One Identity Manager Service.
   - **Workstation | Commandline administration tools**: Enthält verschiedene Kommandozeilenprogramme.
   - **Workstation | Development & Testing**: Enthält die Werkzeuge zur Entwicklung und zum Testen kundenspezifischer Skripte, wie beispielsweise System Debugger.
   - **Workstation | Monitoring**: Enthält Programme zur Überwachung des Systemstatus, wie beispielsweise Job Queue Info.
   - **Server**: Enthält alle Basiskomponenten zur Einrichtung eines Servers.
   - **Server | Jobserver**: Enthält den One Identity Manager Service und die Basisprozesskomponenten. Zusätzliche Maschinenrollen enthalten die Konnektoren zur Synchronisation der einzelnen Zielsysteme.
   - **Server | Jobserver | Configuration tool**: Enthält die Konfigurationswerkzeuge für den One Identity Manager Service.
   - **Database Agent**: Enthält das Programm `DatabaseAgentServiceCmd.exe` zur Ausführung des Database Agent Service über die Kommandozeile.
   - **Documentation**: Enthält die One Identity Manager-Dokumentation in verschiedenen Sprachen.

10. Auf der Seite **WebView2 installieren** werden Sie aufgefordert, Microsoft EdgeWebView2 zu installieren. Die Benutzeroberfläche einiger One Identity Manager-Komponenten benötigt Microsoft EdgeWebView2, um bestimmte Inhalte darstellen zu können.

    HINWEIS: Diese Seite wird nur angezeigt, wenn Sie One Identity Manager-Komponenten installieren möchten, die WebView2 erwarten und WebView2 noch nicht installiert ist.

11. Auf der Seite **Ändern der Service-Einstellungen** können Sie den Namen, den Anzeigenamen und die Beschreibung für die Installation des One Identity Manager Service ändern.

    HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Maschinenrolle **Server | Job Server** ausgewählt haben.

12. Auf der letzten Seite des Installationsassistenten können Sie verschiedene Programme für die weitere Installation starten.
    - Um die Installation des One Identity Manager Schemas auszuführen, starten Sie den Configuration Wizard und folgen Sie den Anweisungen des Configuration Wizard.

      HINWEIS: Führen Sie diesen Schritt nur auf der Arbeitsstation aus, auf der Sie die Installation des One Identity Manager Schemas starten.
    - Um die Konfiguration des One Identity Manager Service zu erstellen, starten Sie das Programm Job Service Configuration.

      HINWEIS: Führen Sie diesen Schritt nur auf Servern aus, auf denen Sie den One Identity Manager Service installiert haben.
13. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.
14. Schließen Sie das Autorun Programm.

One Identity Manager wird für alle Benutzerkonten auf der Arbeitsstation oder dem Server installiert. In der Standardinstallation wird One Identity Manager installiert unter:

- `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen)
- `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)

Verwandte Themen

- Bevor Sie die Installation des One Identity Manager starten auf Seite 53
- Installationsvoraussetzungen auf Seite 22
- Werkzeuge des One Identity Manager auf Seite 14
- One Identity Manager-Komponenten auf Windows Terminalservern installieren auf Seite 56
- Installieren und Konfigurieren einer One Identity Manager-Datenbank auf Seite 58
- Installieren und Konfigurieren des One Identity Manager Service auf Seite 89
- Maschinenrollen und Installationspakete auf Seite 209

One Identity Manager-Komponenten auf Windows Terminalservern installieren

Zur Installation der One Identity Manager-Komponenten auf einem Windows Terminalserver wird vorausgesetzt, dass der Windows Terminalserver vollständig installiert

und konfiguriert wurde. Dies schließt insbesondere das Profilhandling sowie die Berechtigungen zur Benutzung des Windows Terminalservers mit ein.

HINWEIS: Beachten Sie, dass in einer Active Directory Domäne auch der Benutzer selbst die Berechtigung haben muss, den Windows Terminalserver benutzen zu dürfen.

Um die One Identity Manager Komponenten auf einem Windows Terminalserver zu installieren

1. Melden Sie sich mit einem Benutzerkonto, welches über administrative Berechtigungen auf dem Windows Terminalserver verfügt, an.

   Es wird die Anmeldung über eine Konsolenverbindung empfohlen. Dies kann über folgenden Aufruf erfolgen:

   ```
   Start/Ausführen: mstsc /Console /v:<servername>
   mit:
   <servername>: Servername des Terminalservers (ohne führende "\")
   ```

2. Öffnen Sie eine Kommandozeilenkonsole (`CMD.exe`) und schalten Sie den Windows Terminalserver in den Modus zur Softwareinstallation. Dies kann über folgenden Kommandozeilenaufruf erfolgen:

   ```
   CHANGE USER /INSTALL
   ```

3. Starten Sie den Installationsassistenten und installieren die One Identity Manager-Komponenten wie beschrieben.
4. Beenden Sie den Modus zur Softwareinstallation auf dem Windows Terminalserver. Dies kann über folgenden Kommandozeilenaufruf erfolgen:

   ```
   CHANGE USER /EXECUTE
   ```

Nach Abschluss der Installation kann jeder hierzu berechtigte Windows Terminalserver-Benutzer die One Identity Manager-Werkzeuge starten und nutzen.

Weitere Informationen zur Softwareinstallation auf Windows Terminalservern entnehmen Sie der Dokumentation des eingesetzten Windows Betriebssystems.

Verwandte Themen

- One Identity Manager-Komponenten installieren auf Seite 53

Installieren und Konfigurieren einer One Identity Manager-Datenbank

Die One Identity Manager-Datenbank richten Sie mit dem Configuration Wizard ein. Der Configuration Wizard führt die folgenden Schritte aus.

1. Installieren des One Identity Manager Schemas in eine Datenbank.

   Der Configuration Wizard kann eine neue Datenbank erstellen und das One Identity Manager Schema installieren. Alternativ kann das One Identity Manager Schema in eine bereits bestehende Datenbank installiert werden.
2. Erstellen der erforderlichen SQL Server Anmeldungen und Datenbankbenutzer mit den Berechtigungen für den administrative Benutzer, Konfigurationsbenutzer und Endbenutzer.
3. Erstellen der administrativen Systembenutzer und Berechtigungsgruppen.
4. Verschlüsseln der Datenbank.
5. Installieren und Konfigurieren eines One Identity Manager Service mit direktem Zugriff auf die Datenbank für die Verarbeitung von SQL Prozessen und die automatische Softwareaktualisierung der Server.
6. Installieren und Konfigurieren des Database Agent Service.

   Der Database Agent Service steuert die Verarbeitung der DBQueue Prozessor Aufträge. Der Database Agent Service wird über ein Plugin des One Identity Manager Service bereitgestellt. Alternativ kann der Database Agent Service über das Kommandozeilenprogramm `DatabaseAgentServiceCmd.exe` ausgeführt werden.

HINWEIS: Abhängig von der gewählten Edition und den One Identity Manager Modulen können weitere Schritte im Configuration Wizard ausgeführt werden.

Nach der Schemainstallation sind weitere Schritte zur Konfiguration der One Identity Manager-Datenbank erforderlich.

- Konfigurieren Sie die Datenbank für eine Testumgebung, für eine Entwicklungsumgebung oder für den produktiven Einsatz.
- Für die Inbetriebnahme der einzelner Funktionen im One Identity Manager können weitere Systemeinstellungen erforderlich sein.

  Über Konfigurationsparameter konfigurieren Sie die Grundeinstellungen zum Systemverhalten. Der One Identity Manager stellt für verschiedene Konfigurationsparameter Standardeinstellungen zur Verfügung. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

  Die Konfigurationsparameter sind in den One Identity Manager Modulen definiert. Jedes One Identity Manager Modul kann zusätzliche Konfigurationsparameter installieren. Einen Überblick über alle Konfigurationsparameter finden Sie im Designer in der Kategorie **Basisdaten > Allgemein > Konfigurationsparameter**.

- Unter Umständen ist es notwendig, Informationen verschlüsselt in der One Identity Manager-Datenbank abzulegen. Wenn Sie die Datenbank noch nicht während der Installation mit dem Configuration Wizard verschlüsselt haben, dann nutzen Sie das Programm Crypto Configuration zur Verschlüsselung.
- Im One Identity Manager können Datenänderungen sowie Informationen aus der Prozessverarbeitung protokolliert werden. Alle im One Identity Manager protokollierten Aufzeichnungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen. Die Aufzeichnungen sollten in regelmäßigen Abständen aus der One Identity Manager-Datenbank entfernt und archiviert werden.

  Ausführliche Informationen zur Konfiguration der Prozessüberwachung und der Prozesshistorie finden Sie im *One Identity Manager Konfigurationshandbuch*. Ausführliche Informationen zur Archivierung von Daten finden Sie im *One Identity Manager Administrationshandbuch für die Datenarchivierung*.

Detaillierte Informationen zum Thema

- Hinweise zum Einrichten einer One Identity Manager-Datenbank auf Seite 60
- One Identity Manager-Datenbank installieren und konfigurieren auf Seite 61
- Konfigurieren einer One Identity Manager-Datenbank für eine Test-, Entwicklungs- oder Produktivumgebung auf Seite 69
- Verschlüsseln von Datenbankinformationen auf Seite 71
- Lieferantenbenachrichtigung im One Identity Manager auf Seite 78
- Einrichten des E-Mail-Benachrichtigungssystems auf Seite 81

Verwandte Themen

- Minimale Systemanforderungen für den Einsatz von SQL Server als Datenbankserver auf Seite 23
- Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank auf Seite 33
- One Identity Manager-Komponenten installieren auf Seite 53
- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29
- Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36

Hinweise zum Einrichten einer One Identity Manager-Datenbank

- Auf der Arbeitsstation, von welcher die Einrichtung einer One Identity Manager-Datenbank gestartet werden soll, müssen die folgenden Voraussetzungen erfüllt sein:
  - Installation des Configuration Wizard

    Die Installation des Programms erfolgt mit dem Installationsassistenten. Wählen Sie dazu im Installationsassistenten die Maschinenrolle **Workstation** und das Installationspaket **Configuration**.
  - Zugriff auf die Installationsquellen

    HINWEIS: Wenn Sie die Installationsquellen auf ein Ablageverzeichnis kopieren, müssen Sie sicherstellen, dass die relative Verzeichnisstruktur erhalten bleibt.
  - Damit die Kompilierung von HTML-Anwendungen erfolgreich durchgeführt werden kann, müssen Pakete aus dem NPM-Repository heruntergeladen werden. Stellen Sie daher sicher, dass die Arbeitsstation, auf der kompiliert werden soll, eine Verbindung zur Webseite registry.npmjs.org:443 herstellen kann.

    Alternativ ist es möglich, die Pakete von einem Proxy-Server herunterzuladen und manuell zur Verfügung zu stellen.
- Es muss ein Installationsbenutzer mit den Berechtigungen zur Installation einer One Identity Manager-Datenbank zur Verfügung gestellt werden. Wenn Sie für die Installation einer One Identity Manager-Datenbank einen bereits vorhandenen administrativen Benutzer verwenden möchten, stellen Sie sicher, dass dieser Benutzer die erforderlichen Berechtigungen besitzt.

  Ausführliche Informationen finden Sie unter Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29 und Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36.
- Die Verwendung eines Benutzers mit Windows-Authentifizierung für die Installation der Datenbank wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt. Die Aktualisierung der Datenbank muss mit derselben Anmeldung erfolgen.
- Wenn Sie eine das One Identity Manager Schema in eine bestehende Datenbank installieren möchten, stellen Sie sicher, dass die Datenbank die vorausgesetzten Einstellungen hat. Weitere Informationen finden Sie unter Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank auf einem SQL Server auf Seite 25 und Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 34.

- Für eine One Identity Manager-Datenbank auf einem SQL Server wird aus Performancegründen empfohlen, für die Zeit der Schemainstallation die Datenbank auf das Wiederherstellungsmodell **Einfach** zu setzen.
- Starten Sie den Configuration Wizard immer auf einer administrativen Arbeitsstation.
- Das Programm führt eine Remote-Installation des One Identity Manager Service aus.
- Wenn Sie den Configuration Wizard auf einem Server starten, auf dem Sie auch einen One Identity Manager Service konfigurieren wollen, so überspringen Sie den Schritt zum Installieren eines Dienstservers für den lokalen Server im Configuration Wizard. Installieren Sie den One Identity Manager Service in diesem Fall mit dem Installationsassistenten. Weitere Informationen finden Sie unter Installieren und Konfigurieren des One Identity Manager Service auf Seite 89.
- Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, beachten Sie die Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77.

One Identity Manager-Datenbank installieren und konfigurieren

WICHTIG: Starten Sie den Configuration Wizard immer auf einer administrativen Arbeitsstation. Wenn Sie den Configuration Wizard auf einem Server starten, auf dem Sie auch einen One Identity Manager Service konfigurieren wollen, so überspringen Sie den Schritt zum Installieren eines Dienstservers für den lokalen Server im Configuration Wizard.

Um eine Datenbank im Configuration Wizard zu installieren

1. Starten Sie den Configuration Wizard.
2. Auf der Startseite des Configuration Wizard wählen Sie die Option **Datenbank erstellen und installieren** und klicken Sie **Weiter**.
3. Um eine neue Datenbank zu installieren, erfassen Sie auf der Seite **Administrative Datenbankverbindung herstellen** folgende Verbindungsdaten zur Datenbank.
   - **Server**: Datenbankserver.
   - (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
   - **Nutzer**: SQL Server Anmeldename des Installationsbenutzer.
   - **Kennwort**: Kennwort für den Installationsbenutzer.

   - ODER -

   Um eine bestehende leere Datenbank zu verwenden, aktivieren Sie auf der Seite **Administrative Datenbankverbindung herstellen** die Option **Eine bereits**

existierende leere Datenbank verwenden und erfassen Sie die Verbindungsdaten zur Datenbank.

- **Server**: Datenbankserver.
- (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
- **Nutzer**: SQL Server Anmeldename des Installationsbenutzer.
- **Kennwort**: Kennwort für den Installationsbenutzer.
- **Datenbank**: Name der Datenbank.

TIPP: Um zusätzliche Verbindungsoptionen zu konfigurieren, aktivieren Sie die Option **Erweitert**.

4. Wenn Sie eine neue Datenbank erstellen, führen Sie auf der Seite **Datenbank erstellen** folgende Aktionen aus.
   a. Erfassen Sie im Bereich **Datenbankeigenschaften** die folgenden Informationen zur Datenbank.

Tabelle 15: Datenbankeigenschaften

Eingabe	Beschreibung
Datenbankname	Name der Datenbank.
Datenverzeichnis	Verzeichnis, in dem die Datendatei erstellt wird. Zur Auswahl stehen: • **<Standard>**: Standardverzeichnis des Datenbankservers. • **<browse>**: Wählen Sie ein Verzeichnis über den Dateibrowser. • **<Verzeichnisangabe>**: Verzeichnis, in dem bereits Datendateien installiert sind.
Log Verzeichnis	Verzeichnis, in dem die Transaktionsprotokolldatei erstellt wird. Zur Auswahl stehen: • **<Standard>**: Standardverzeichnis des Datenbankservers. • **<browse>**: Wählen Sie ein Verzeichnis über den Dateibrowser. • **<Verzeichnisangabe>**: Verzeichnis, in dem bereits Transaktionsprotokolldateien installiert sind.

Eingabe	Beschreibung
RAM-Tabellen Verzeichnis	Verzeichnis für Datendateigruppe und Datenbankdatei für speicheroptimierte Tabellen. Zur Auswahl stehen: • **<Standard>**: Standardverzeichnis des Datenbankservers. • **<browse>**: Wählen Sie ein Verzeichnis über den Dateibrowser. • **<Verzeichnisangabe>**: Verzeichnis, in dem bereits Datendateien für speicheroptimierte Tabellen installiert sind.
Initiale Größe	Anfangsgröße der Datenbankdateien. Zur Auswahl stehen: • **<Standard>**: Standardvorgabe des Datenbankservers. • **<custom>**: Freie Eingabe. • Verschiedene empfohlene Größen: Abhängig von der Anzahl der Personen, die verwaltet werden.

b. Wählen Sie im Bereich **Installationsquellen** das Verzeichnis mit den Installationsdateien.

- ODER -

Wenn Sie eine bestehende Datenbank verwenden, wählen Sie auf der Seite **Datenbank erstellen** im Bereich **Installationsquellen** das Verzeichnis mit den Installationsdateien.

5. Auf der Seite **Konfigurationsmodule auswählen** wählen Sie die Konfigurationsmodule.
   - Wenn Sie den Configuration Wizard über den Installationsassistenten gestartet haben, sind die Konfigurationsmodule für die gewählte Edition bereits aktiviert. Prüfen Sie in diesem Fall die Modulauswahl.
   - Wenn Sie den Configuration Wizard direkt gestartet haben, wählen Sie an dieser Stelle die Konfigurationsmodule. Abhängige Konfigurationsmodule werden automatisch mit ausgewählt.
6. Auf der Seite **Datenbanküberprüfung** werden Fehler angezeigt, die eine Verarbeitung der Datenbank verhindern. Beheben Sie die Fehler bevor Sie mit der Installation fortfahren.
7. Auf der Seite **Neue Anmeldung für administrative Benutzer erstellen** entscheiden Sie, welche SQL Server Anmeldung für administrative Benutzer verwendet wird. Zur Auswahl stehen:

- **Neue SQL Server Anmeldungen für die Datenbank erstellen**: Wählen Sie diese Option, wenn Sie mit dem abgestuften Berechtigungskonzept arbeiten möchten.

  Es wird für die Datenbank eine neue, administrative Anmeldung auf dem SQL Server erstellt.

  - Erfassen Sie den Anmeldenamen, das Kennwort und die Kennwortbestätigung für die neue SQL Server Anmeldung.

  Im weiteren Verlauf werden mit dem Configuration Wizard zusätzliche SQL Server Anmeldungen für Konfigurationsbenutzer und für Endbenutzer erstellt.
- **Eine existierende SQL Server Anmeldung verwenden**: Wählen Sie diese Option, wenn Sie bereits eine administrative SQL Server Anmeldung erstellt haben und diese verwenden möchten. Im weiteren Verlauf werden mit dem Configuration Wizard zusätzliche SQL Server Anmeldungen für Konfigurationsbenutzer und für Endbenutzer erstellt.

  a. Erfassen Sie den Anmeldenamen, das Kennwort und die Kennwortbestätigung für die SQL Server Anmeldung.

  b. Aktivieren Sie die Option **Berechtigungen** damit die SQL Server Anmeldung Berechtigungen auf die Datenbank erhält. Wenn die Option deaktiviert ist, erfolgt nur eine Prüfung der Berechtigungen.
- **Aktuelle SQL Server Anmeldung für die Datenbank verwenden**: Wenn Sie diese Option wählen, werden keine zusätzlichen SQL Server Anmeldungen für die Datenbank erstellt. In diesem Fall kann nicht mit dem abgestuften Berechtigungskonzept auf SQL-Ebene gearbeitet werden. Es wird der Benutzer verwendet, den Sie für die Verbindung zur Datenbank angegeben haben.

  HINWEIS: Wenn Sie zu einem späteren Zeitpunkt zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

8. Auf der Seite **Verarbeitung der Datenbank** werden die Installationsschritte angezeigt.

   Die Installation und Konfiguration der Datenbank wird durch den Configuration Wizard automatisch durchgeführt. Der Vorgang kann abhängig von Datenumfang und Systemperformance einige Zeit dauern. Nach Abschluss der Verarbeitung, klicken Sie **Weiter**.

   TIPP: Um detaillierte Informationen zu den Verarbeitungsschritten und zum Migrationsprotokoll zu erhalten, aktivieren Sie die Option **Erweitert**.

9. Auf der Seite **Neue Anmeldungen für Konfigurationsbenutzer und Endbenutzer erstellen** erfassen Sie die den Anmeldenamen, das Kennwort und die Kennwortbestätigung für die SQL Server Anmeldungen für Konfigurationsbenutzer und Endbenutzer.

   HINWEIS: Das Kennwort muss den Anforderungen der Windows Richtlinien für Kennwörter entsprechen.

10. Auf der Seite **Systeminformationen** erfassen Sie die Kundenformationen und erstellen Sie administrative Systembenutzer für den One Identity Manager.
    a. Im Bereich **Kundeninformation** erfassen Sie den vollständigen Namen des Unternehmens.
    b. Im Bereich **Systembenutzer** konfigurieren Sie die vordefinierten administrativen Systembenutzer und erfassen eigene administrative Systembenutzer.
        - Für die vordefinierten Systembenutzer erfassen Sie ein Kennwort und die Kennwortbestätigung.
        - Um kundenspezifische Systembenutzer zu erstellen, klicken Sie die Schaltfläche + und erfassen Sie die Bezeichnung, Kennwort und Kennwortwiederholung.

        TIPP: Über die Schaltfläche **<...>** neben der Bezeichnung eines Systembenutzers konfigurieren Sie weitere Einstellungen für den Systembenutzer. Diese Einstellungen können Sie auch zu einem späteren Zeitpunkt im Designer anpassen.
    c. (Optional) Erstellen Sie kundenspezifische Berechtigungsgruppen.

        Durch den Configuration Wizard werden bereits kundenspezifische Berechtigungsgruppen erzeugt, die Sie für die Definition von Berechtigungen auf eventuelle kundenspezifische Schemaerweiterungen 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.

        Um weitere Berechtigungsgruppen zu erstellen

        i. Aktivieren Sie die Option **Erweitert** und klicken Sie im Bereich **Berechtigungsgruppen** die Schaltfläche +.
        ii. Erfassen Sie die Bezeichnung der Berechtigungsgruppe. Kennzeichnen Sie eigene Berechtigungsgruppen mit dem Präfix **CCC**.
        iii. Für rollenbasierte Berechtigungsgruppen aktivieren Sie die Option **Rollenbasiert**.
11. Auf der Seite **Datenbankverschlüsselung aktivieren** wählen Sie eine der folgenden Optionen.
    - **Datenbank unverschlüsselt lassen**: Die Datenbank wird nicht verschlüsselt. Sie können die Datenbank zu einem späteren Zeitpunkt mit dem Programm Crypto Configuration verschlüsseln.
    - **Datenbankverschlüsselung aktivieren**: Die Datenbank wird im nächsten Schritt verschlüsselt.

1. Geben Sie im Eingabefeld **Privater Schlüssel** den Namen der Schlüsseldatei (Standard: `private.key`) ein.
2. Klicken Sie **Neu** und wählen Sie über den Dateibrowser den Ablagepfad für die Schlüsseldatei.
3. Klicken Sie **Speichern**.

   Die Schlüsseldatei (`*.key`) wird erzeugt. Der Dateibrowser wird geschlossen. Pfad und Dateiname werden unter **Privater Schlüssel** angezeigt.
4. Bestätigen Sie, dass Sie die Schlüsseldatei gesichert haben.

   Beachten Sie die Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77.

12. Auf der Seite **Dienstinstallation** können Sie bereits einen Jobserver für den Server erzeugen, auf dem die One Identity Manager-Datenbank installiert ist.

    HINWEIS: Wenn Sie zu diesem Zeitpunkt noch keinen Jobserver mit One Identity Manager Service einrichten möchten, aktivieren Sie die Option **Keinen Dienst installieren**.

    a. Erfassen Sie im Bereich **Installationsinformationen** folgende Informationen um den One Identity Manager Service zu installieren.
       - **Computer**: Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
       - **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

       Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen erfassen. Weitere Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

    b. Im Bereich **Maschinenrollen** wählen Sie die Maschinenrollen für den Dienst. Standardmäßig ist die Maschinenrolle **Server | Jobserver** festgelegt. Sie können weitere Maschinenrollen hinzufügen.

    c. (Optional) Aktivieren Sie die Option **Erweitert** und prüfen Sie im Bereich **Konfiguration** die Konfiguration des One Identity Manager Service.

       HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des One Identity Manager Service finden Sie im *One Identity Manager Konfigurationshandbuch*.

    d. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.

HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.

13. Die Seite **Datenbankaufgaben verarbeiten** wird nur angezeigt, wenn noch Aufträge für den DBQueue Prozessor in der DBQueue bereitstehen, die während der Installation der Datenbank verarbeitet werden müssen. Nach Abschluss der Verarbeitung, klicken Sie **Weiter**.
14. Auf der letzten Seite des Configuration Wizard klicken Sie **Fertig**.

Verwandte Themen

- Hinweise zum Einrichten einer One Identity Manager-Datenbank auf Seite 60
- Fehlermeldungen bei der Installation und der Aktualisierung der One Identity Manager-Datenbank auf Seite 190
- Verarbeiten der One Identity Manager-Datenbank während der Einrichtung mit dem Configuration Wizard auf Seite 67
- Verschlüsseln von Datenbankinformationen auf Seite 71
- Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77

Verarbeiten der One Identity Manager-Datenbank während der Einrichtung mit dem Configuration Wizard

Die Installation und Konfiguration der One Identity Manager-Datenbank wird durch den Configuration Wizard automatisch durchgeführt. Der Configuration Wizard kann eine neue Datenbank erstellen und das One Identity Manager Schema installieren. Alternativ kann das One Identity Manager Schema in eine bereits bestehende Datenbank installiert werden.

Der Configuration Wizard führt bei der Verarbeitung der Datenbank die folgenden Schritte aus:

- Erstellen der erforderlichen SQL Server Anmeldungen und Datenbankbenutzer mit den Berechtigungen für den administrativen Benutzer, den Konfigurationsbenutzer und Endbenutzer. Weitere Informationen finden Sie unter Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29.
- Installieren des One Identity Manager Schemas.

Vor der Schemainstallation prüft der Configuration Wizard die Datenbank. Die Fehlermeldungen werden in einem separaten Meldungsfenster ausgegeben. Die Fehler sind manuell zu korrigieren. Erst danach kann die Schemainstallation gestartet werden.

Durch die Schemainstallation werden alle benötigten Tabellen, Datentypen, Datenbankprozeduren in die Datenbank eingespielt. Die gewählten Editionen und Konfigurationsmodule werden aktiviert. Während einer Schemainstallation werden Berechnungsaufträge in die Datenbank eingestellt. Diese werden durch den DBQueue Prozessor verarbeitet.

Bei einer Schemainstallation mit dem Configuration Wizard werden das Migrationsdatum und der Migrationsstand in der Transporthistorie der Datenbank aufgezeichnet.

- Kompilieren des Systems.

  Es werden die Skripte, Bildungsregeln und Prozesse in der Datenbank bekannt gegeben. Es wird das Authentifizierungsmodul **Systembenutzer** mit dem Systembenutzer **viadmin** zum Kompilieren verwendet.

- Laden der Dateien für die automatische Softwareaktualisierung.

  Um die Dateien des One Identity Manager über die Mechanismen der automatischen Softwareaktualisierung zu verteilen, werden die Dateien in die One Identity Manager-Datenbank geladen.

- Erstellen der administrativen Systembenutzer und Berechtigungsgruppen.

  Für die Authentifizierung am One Identity Manager wird ein Systembenutzer benötigt. One Identity Manager stellt verschiedene Systembenutzer bereit, deren Berechtigungen auf die verschiedenen Aufgaben abgestimmt sind. Ausführliche Informationen zu Systembenutzern, Berechtigungsgruppen und zur Vergabe von Berechtigungen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

  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.

  Die kundenspezifischen Systembenutzer werden durch den Configuration Wizard als administrative Systembenutzer erstellt. Administrative Systembenutzer werden automatisch in alle nicht-rollenbasierten Berechtigungsgruppen aufgenommen und erhalten alle Berechtigungen des Systembenutzers **viadmin**.

- Installieren und Konfigurieren eines One Identity Manager Service mit direktem Zugriff auf die Datenbank für die Verarbeitung von SQL Prozessen und die automatische Softwareaktualisierung der Server

  Die Verarbeitung der definierten Prozesse erfolgt über den One Identity Manager Service. Zur Prozessverarbeitung muss der Dienst auf den Servern des One Identity

Manager-Netzwerkes installiert sein. Die Server müssen in der One Identity Manager-Datenbank als Jobserver bekannt gegeben werden.

Während der initialen Schemainstallation mit dem Configuration Wizard wird in der One Identity Manager-Datenbank bereits ein Jobserver für den Server erzeugt, auf dem die One Identity Manager-Datenbank installiert ist. Dieser Jobserver erhält die Serverfunktionen **SQL Ausführungsserver** und **Aktualisierungsserver**.

- Der SQL Ausführungsserver übernimmt die Verarbeitung von SQL Prozessen.
- Der Aktualisierungsserver sorgt für die automatische Softwareaktualisierung der weiteren Server.

Der SQL Ausführungsserver und der Aktualisierungsserver benötigen zur Verarbeitung der Prozesse eine direkte Verbindung zur One Identity Manager-Datenbank. Mit dem Configuration Wizard installieren Sie auf einem Server den One Identity Manager Service, um diese Prozesse zu verarbeiten.

Der Configuration Wizard führt folgende Schritte aus:

- Installieren der One Identity Manager Service Komponenten
- Konfigurieren des One Identity Manager Service
- Starten des One Identity Manager Service

- Installieren und Konfigurieren des Database Agent Service.

  Der Database Agent Service steuert die Verarbeitung der DBQueue Prozessor Aufträge. Der Database Agent Service wird über ein Plugin des One Identity Manager Service bereitgestellt. Alternativ kann der Database Agent Service über das Kommandozeilenprogramm `DatabaseAgentServiceCmd.exe` ausgeführt werden.

  HINWEIS: Wenn der Database Agent Service nicht arbeitet, wird in allen Administrationswerkzeugen eine Meldung in der Statuszeile angezeigt. Um diese Meldung zu sehen, benötigen die Benutzer mindestens die Berechtigungsebene für Konfigurationsbenutzer.

Verwandte Themen

- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- Transporthistorie anzeigen und One Identity Manager Version prüfen auf Seite 188

Konfigurieren einer One Identity Manager-Datenbank für eine Test-, Entwicklungs- oder Produktivumgebung

Über die Staging-Ebene der One Identity Manager-Datenbank legen Sie fest, ob es sich um eine Testdatenbank, Entwicklungsdatenbank oder produktive Datenbank handelt. Über die Staging-Ebene werden einige Datenbankeinstellungen gesteuert.

Wenn Sie die Staging-Ebene der Datenbank ändern, werden die folgenden Einstellungen konfiguriert.

Tabelle 16: Standardeinstellungen für Entwicklungsumgebung, Testumgebung und Produktivumgebung

Einstellung	Entwicklungsumgebung	Testumgebung	Produktivumgebung
Farbe der Statuszeile der One Identity Manager-Werkzeuge	keine	Grün	Gelb
Maximale Laufzeit DBQueue Prozessor	20 Minuten	40 Minuten	120 Minuten
Maximale Anzahl der Slots für DBQueue Prozessor	5	7	Maximale Anzahl der Slots laut Hardwarekonfiguration

Um die Staging-Ebene einer Datenbank anzupassen

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Staging Ebene der Datenbank** und klicken Sie **Starten**.

   Der Designer wird gestartet.
3. Wählen Sie im Designer die Kategorie **Basisdaten > Allgemein > Datenbanken**.
4. Wählen Sie im Listeneditor die Datenbank.
5. Wählen Sie in der Bearbeitungsansicht den Tabreiter **Allgemein**.
6. Ändern Sie den Wert der Eigenschaft **Staging Ebene** auf **Testumgebung**, **Entwicklungssystem** oder **Produktivsystem**.
7. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
8. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Die Standardeinstellungen für den DBQueue Prozessor sind für einen Normalbetrieb ausgelegt und müssen in der Regel nicht angepasst werden.

Wenn mehrere Datenbanken in einer verwalteten Instanz in Azure SQL-Datenbank betrieben werden, können Sie die Anzahl der Slots fest vorgeben. Passen Sie im Designer den folgenden Konfigurationsparameter an.

- **QBM | DBServerAgent | CountSlotAgents**: Genaue Anzahl der Slots. Ist der Konfigurationsparameter aktiviert, wird immer die Anzahl der angegebenen Slot

eingerichtet. Es erfolgt keine interne Berechnung der Slotanzahl anhand der Hardwarekonfiguration. Die Änderung der Konfiguration des Servers hat keinen Einfluss. Es wird der Wert **15** empfohlen.

HINWEIS: Für den Einsatz einer Datenbank auf einem SQL Server wird der Konfigurationsparameter nicht empfohlen. Für den Einsatz einer Datenbank auf einem SQL Server hat sich die Ermittlung der Slots über die Hardwarekonfiguration bewährt.

Für Testumgebungen und Entwicklungsumgebungen sind die Konfigurationseinstellungen reduziert, da sich mehrere Datenbanken auf einem Server befinden können. Müssen aus Performancegründen die Einstellungen für Testumgebungen und Entwicklungsumgebungen angepasst werden, ändern Sie im Designer die Einstellungen der folgenden Konfigurationsparameter an.

- **QBM | DBQueue | CountSlotsMax**: Anzahl der maximal zu verwendenden Slots.

  Nutzen Sie den Konfigurationsparameter um die Anzahl der Slots bei Bedarf zu reduzieren. Werte kleiner als **5** sind nicht zulässig.

  Ausnahme: Für die Nutzung der maximal verfügbaren Slots laut Hardwarekonfiguration geben Sie den Wert **0** an.
- **QBM | DBQueue | KeepAlive**: Maximale Laufzeit des zentralen Dispatchers. Nach Ablauf der Laufzeit werden die Aufträge aktuell verwendeter Slots noch abgearbeitet. Anschließend werden die Slots gestoppt und der zentrale Dispatcher beendet.

  Der minimal zulässige Wert für die Laufzeit ist **5 Minuten**, der maximal zulässige Wert ist **720 Minuten**.

Ausführliche Informationen zur Arbeitsweise des DBQueue Prozessor finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verschlüsseln von Datenbankinformationen

HINWEIS: Es wird empfohlen, vor der Verschlüsselung der Datenbankinformationen eine Datenbanksicherung zu erstellen, um im Bedarfsfall den vorherigen Zustand wieder herstellen zu können.

Unter Umständen ist es notwendig, Informationen verschlüsselt in der One Identity Manager-Datenbank abzulegen. Wenn Sie die Datenbank noch nicht während der Installation mit dem Configuration Wizard verschlüsselt haben, dann nutzen Sie das Programm Crypto Configuration zur Verschlüsselung. Mit diesem Programm wird eine Schlüsseldatei erzeugt und die Inhalte der betroffenen Datenbankspalten werden konvertiert.

Um das Verschlüsselungsverfahren festzulegen

- Aktivieren Sie im Designer den Konfigurationsparameter **Common | EncryptionScheme** und wählen Sie eine der Optionen:

- **RSA**: RSA-Verschlüsselung mit AES für größere Daten (Standard).
- **FIPSCompliantRSA**: FIPS zertifizierter RSA mit AES für größere Daten. Das Verfahren ist einzusetzen, wenn die Verschlüsselung dem FIPS 140-2 Standard entsprechen muss. Die lokale Sicherheitsrichtlinie **Use FIPS compliant algorithms for encryption, hashing, and signing** muss aktiviert sein.

HINWEIS: Ist der Konfigurationsparameter **Common | EncryptionScheme** nicht aktiviert, wird die RSA-Verschlüsselung als Verfahren genutzt.

Detaillierte Informationen zum Thema

- Neuen Datenbankschlüssel erzeugen und Datenbankinformationen verschlüsseln auf Seite 72
- Datenbankschlüssel ändern und Datenbankinformationen verschlüsseln auf Seite 73
- Datenbankinformationen erneut verschlüsseln auf Seite 75
- Datenbankinformationen entschlüsseln auf Seite 76
- Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77

Neuen Datenbankschlüssel erzeugen und Datenbankinformationen verschlüsseln

HINWEIS: Es wird empfohlen, vor der Verschlüsselung der Datenbankinformationen eine Datenbanksicherung zu erstellen, um im Bedarfsfall den vorherigen Zustand wieder herstellen zu können.

Um einen neuen Datenbankschlüssel zu erzeugen und die One Identity Manager-Datenbank zu verschlüsseln

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Datenbank verschlüsseln** und klicken Sie **Starten**.

   Das Programm Crypto Configuration wird gestartet.
3. Auf der Startseite klicken Sie **Weiter**.
4. Auf der Seite **Herstellen der Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
5. Auf der Seite **Auswahl der Aktion** wählen Sie **Erzeugen oder Ändern eines Datenbankschlüssels**.
6. Auf der Seite **Privater Schlüssel** wählen Sie **Bisher war keine Verschlüsselung aktiviert**.
7. Auf der Seite **Neuer privater Schlüssel** erzeugen Sie einen neuen Schlüssel.

a. Klicken Sie **Erzeuge Schlüssel**.

b. Wählen Sie über den Dateibrowser den Ablagepfad und geben Sie den Namen der Schlüsseldatei ein.

c. Klicken Sie **Speichern**.

   Die Schlüsseldatei (`*.key`) wird erzeugt. Der Dateibrowser wird geschlossen. Pfad und Dateiname werden unter **Privater Schlüssel** angezeigt.

d. Klicken Sie **Weiter**.

   Die zu verschlüsselnden Daten werden ermittelt.

8. Auf der Seite **Konvertiere Datenbank** werden die zu verschlüsselnden Daten angezeigt.

   a. Klicken Sie **Konvertiere**.

   b. Bestätigen Sie die folgenden zwei Sicherheitsabfragen mit **Ja**.

      Die Verschlüsselung der Daten wird gestartet. Der Fortschritt der Konvertierung wird angezeigt.

   c. Klicken Sie **Weiter**.

9. Auf der letzten Seite klicken Sie **Fertig**, um das Programm zu beenden.

Verwandte Themen

- Datenbankschlüssel ändern und Datenbankinformationen verschlüsseln auf Seite 73
- Datenbankinformationen erneut verschlüsseln auf Seite 75
- Datenbankinformationen entschlüsseln auf Seite 76
- Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77

Datenbankschlüssel ändern und Datenbankinformationen verschlüsseln

HINWEIS:

- Um einen Datenbankschlüssel zu ändern, benötigen Sie die Schlüsseldatei mit dem alten Datenbankschlüssel. Der Schlüssel wird geändert und in einer neuen Schlüsseldatei gespeichert.
- Es wird empfohlen, vor der Verschlüsselung der Datenbankinformationen eine Datenbanksicherung zu erstellen, um im Bedarfsfall den vorherigen Zustand wieder herstellen zu können.

Um einen Datenbankschlüssel zu ändern und die One Identity Manager-Datenbank zu verschlüsseln

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Datenbank verschlüsseln** und klicken Sie **Starten**.

   Das Programm Crypto Configuration wird gestartet.
3. Auf der Startseite klicken Sie **Weiter**.
4. Auf der Seite **Herstellen der Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
5. Auf der Seite **Auswahl der Aktion** wählen Sie **Erzeugen oder Ändern eines Datenbankschlüssels**.
6. Auf der Seite **Privater Schlüssel** laden Sie den vorhandenen Schlüssel.
   a. Wählen Sie **Die Verschlüsselung war aktiviert**.
   b. Klicken Sie **Lade Schlüssel**.
   c. Wählen Sie über den Dateibrowser die Datei (`*.key`) mit dem alten Datenbankschlüssel.
   d. Klicken Sie **Öffnen**.

      Der Dateibrowser wird geschlossen. Pfad und Dateiname werden angezeigt.
   e. Klicken Sie **Weiter**.
7. Auf der Seite **Neuer privater Schlüssel** erzeugen Sie einen neuen Schlüssel.
   a. Klicken Sie **Erzeuge Schlüssel**.
   b. Wählen Sie über den Dateibrowser den Ablagepfad und geben Sie den Namen der Schlüsseldatei ein.
   c. Klicken Sie **Speichern**.

      Die Schlüsseldatei (`*.key`) wird erzeugt. Der Dateibrowser wird geschlossen. Pfad und Dateiname werden unter **Privater Schlüssel** angezeigt.
   d. Klicken Sie **Weiter**.

      Die zu verschlüsselnden Daten werden ermittelt.
8. Auf der Seite **Konvertiere Datenbank** werden die zu verschlüsselnden Daten angezeigt.
   a. Klicken Sie **Konvertiere**.
   b. Bestätigen Sie die folgenden zwei Sicherheitsabfragen mit **Ja**.

      Die Verschlüsselung der Daten wird gestartet. Der Fortschritt der Konvertierung wird angezeigt.
   c. Klicken Sie **Weiter**.
9. Auf der letzten Seite klicken Sie **Fertig**, um das Programm zu beenden.

Verwandte Themen

- Neuen Datenbankschlüssel erzeugen und Datenbankinformationen verschlüsseln auf Seite 72
- Datenbankinformationen erneut verschlüsseln auf Seite 75
- Datenbankinformationen entschlüsseln auf Seite 76
- Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77

Datenbankinformationen erneut verschlüsseln

Verwenden Sie dieses Verfahren, wenn die Datenbank bereits verschlüsselt ist und Sie weitere Datenbankspalten verschlüsseln möchten.

HINWEIS: Es wird empfohlen, vor der Verschlüsselung der Datenbankinformationen eine Datenbanksicherung zu erstellen, um im Bedarfsfall den vorherigen Zustand wieder herstellen zu können.

Um die One Identity Manager-Datenbank mit einem vorhandenen Datenbankschlüssel erneut zu verschlüsseln

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Datenbank verschlüsseln** und klicken Sie **Starten**.

   Das Programm Crypto Configuration wird gestartet.
3. Auf der Startseite klicken Sie **Weiter**.
4. Auf der Seite **Herstellen der Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
5. Auf der Seite **Auswahl der Aktion** wählen Sie **Verschlüsselung mittels des bestehenden Schlüssels**.

   Die zu verschlüsselnden Daten werden ermittelt.
6. Auf der Seite **Konvertiere Datenbank** werden die zu verschlüsselnden Daten angezeigt.
   a. Klicken Sie **Konvertiere**.
   b. Bestätigen Sie die folgenden zwei Sicherheitsabfragen mit **Ja**.

      Die Verschlüsselung der Daten wird gestartet. Der Fortschritt der Konvertierung wird angezeigt.
   c. Klicken Sie **Weiter**.
7. Auf der letzten Seite klicken Sie **Fertig**, um das Programm zu beenden.

Verwandte Themen

- Neuen Datenbankschlüssel erzeugen und Datenbankinformationen verschlüsseln auf Seite 72
- Datenbankschlüssel ändern und Datenbankinformationen verschlüsseln auf Seite 73
- Datenbankinformationen entschlüsseln auf Seite 76
- Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77

Datenbankinformationen entschlüsseln

HINWEIS:

- Sie benötigen Sie die Datei mit dem Datenbankschlüssel.
- Es wird empfohlen, vor der Verschlüsselung der Datenbankinformationen eine Datenbanksicherung zu erstellen, um im Bedarfsfall den vorherigen Zustand wieder herstellen zu können.

Um die One Identity Manager-Datenbank zu entschlüsseln

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Datenbank verschlüsseln** und klicken Sie **Starten**.

   Das Programm Crypto Configuration wird gestartet.
3. Auf der Startseite klicken Sie **Weiter**.
4. Auf der Seite **Herstellen der Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
5. Auf der Seite **Auswahl der Aktion** wählen Sie **Entschlüsselung der Daten**.

   Die zu entschlüsselnden Daten werden ermittelt.
6. Auf der Seite **Konvertiere Datenbank** werden die zu entschlüsselnden Daten angezeigt.
   a. Klicken Sie **Konvertiere**.
   b. Bestätigen Sie die folgenden zwei Sicherheitsabfragen mit **Ja**.
   c. Wählen Sie über den Dateibrowser die Datei (`*.key`) mit dem Datenbankschlüssel.
   d. Klicken Sie **Öffnen**.

      Der Dateibrowser wird geschlossen. Die Entschlüsselung der Daten wird gestartet. Der Fortschritt der Konvertierung wird angezeigt.
   e. Klicken Sie **Weiter**.
7. Auf der letzten Seite klicken Sie **Fertig**, um das Programm zu beenden.

Verwandte Themen

- Neuen Datenbankschlüssel erzeugen und Datenbankinformationen verschlüsseln auf Seite 72
- Datenbankschlüssel ändern und Datenbankinformationen verschlüsseln auf Seite 73
- Datenbankinformationen erneut verschlüsseln auf Seite 75
- Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77

Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank

Wenn Sie die One Identity Manager-Datenbank verschlüsseln, müssen Sie dem One Identity Manager Service den Datenbankschlüssel bekanntgeben.

VORSICHT: Wenn der One Identity Manager Service beim Start einen privaten Schlüssel im Installationsverzeichnis findet, so legt er diesen im Windows internen Schlüsselcontainer seines Dienstkontos ab und löscht die Datei auf der Festplatte. Sichern Sie daher den privaten Schlüssel zusätzlich an einer anderen Stelle als dem Installationsverzeichnis des Dienstes!

WICHTIG:

- Die Datei mit dem privaten Schlüssel muss auf allen Servern mit aktivem One Identity Manager Service im Installationsverzeichnis des Dienstes vorhanden sein.
- Wenn Sie das Benutzerkonto des One Identity Manager Service ändern, müssen Sie die Schlüsseldatei neu im Installationsverzeichnis des Dienstes ablegen.

Um den Datenbankschlüssel bekanntzugeben

1. Geben Sie in der Konfigurationsdatei des One Identity Manager Service folgenden Informationen bekannt. Verwenden Sie den Jobservereditor im Designer oder das Programm Job Service Configuration zur Bearbeitung der Konfigurationsdatei. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Tabelle 17: Konfiguration des One Identity Manager Service für die Verschlüsselung

Konfigurationsmodul	Parameter	Bedeutung
JobServiceDestination	Verschlüsselungsverfahren (`EncryptionScheme`)	Eingesetztes Verschlüs-selungsverfahren.
JobServiceDestination	Datei mit privatem	Datei mit dem privaten

Konfigurationsmodul	Parameter	Bedeutung
	Schlüssel (`PrivateKey`)	Schlüssel. Standardwert ist `private.key`.
JobServiceDestination	ID des privaten Schlüssels (`PrivateKeyId`)	ID des privaten Schlüssels. Verwenden Sie den Parameter, wenn Sie mit mehreren privaten Schlüsseln arbeiten, beispielsweise wenn der One Identity Manager Service Daten zwischen zwei verschlüsselten One Identity Manager-Datenbanken übertragen muss. Ist keine ID angegeben, wird nach der Datei `private.key` gesucht.
Datei mit privatem Schlüssel		ID des privaten Schlüssel und Pfad zur privaten Schlüsseldatei. Die ID wird in der JobServiceDestination im Parameter **ID des privaten Schlüssels** (`PrivateKeyId`) erwartet. Der Standardschlüssel hat die ID **Default**.

2. Legen Sie die erzeugte Schlüsseldatei im Installationsverzeichnis des Dienstes ab.
3. Öffnen Sie die Dienstverwaltung und starten Sie den One Identity Manager Service neu.

Detaillierte Informationen zum Thema

- Verschlüsseln von Datenbankinformationen auf Seite 71

Lieferantenbenachrichtigung im One Identity Manager

Geben Sie uns die Gelegenheit, Sie auf dem Laufenden zu halten. Die Schnittstellen zu anderen Systemen werden kontinuierlich weiterentwickelt. Aktivieren Sie

Lieferantenbenachrichtigungen, um Nachrichten über wichtige Programmaktualisierungen für Ihr System zu erhalten.

Wenn die Lieferantenbenachrichtigung aktiviert ist, erzeugt One Identity Manager einmal im Monat eine Liste der Systemeinstellungen und sendet die Liste an One Identity. Diese Liste enthält keine personenbezogenen Daten. Die Liste wird von unserem Kunden-Support-Team proaktiv überprüft, welches nach wesentlichen Änderungen schaut um mögliche Probleme zu identifizieren bevor sie sich auf Ihrem System verwirklichen. Die Listen können von unseren F&E-Mitarbeitern für die Analyse, Diagnose und Replikation zu Testzwecken verwendet werden. Diese Informationen behalten Gültigkeit, solange Ihr Unternehmen weiterhin Pflegeleistungen für dieses Produkt bezieht.

HINWEIS: Sie können die aktuellsten Systeminformationen jederzeit aus dem Menü **Hilfe > Info** überprüfen.

Detaillierte Informationen zum Thema

- Lieferantenbenachrichtigung aktivieren auf Seite 79
- Lieferantenbenachrichtigung prüfen auf Seite 80
- Lieferantenbenachrichtigung deaktivieren auf Seite 80

Lieferantenbenachrichtigung aktivieren

HINWEIS: Die Lieferantenbenachrichtigung können Sie im Launchpad nur auf einer One Identity Manager-Datenbank mit der Staging-Ebene **Produktivumgebung** konfigurieren.

Voraussetzung für die Lieferantenbenachrichtigung

- Im One Identity Manager ist ein Jobserver als SMTP Host für den Mailversand konfiguriert.
- Die Konfigurationsparameter für die E-Mail-Benachrichtigung sind konfiguriert.

Um die Lieferantenbenachrichtigung zu aktivieren

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Lieferantenbenachrichtigung konfigurieren** und klicken Sie **Starten**.

   Der Designer wird gestartet und der Konfigurationsparametereditor geöffnet.
3. Aktivieren Sie den Konfigurationsparameter **Common | MailNotification | VendorNotification** und tragen Sie die E-Mail-Adresse Ihres Unternehmenskontaktes ein.

   Die E-Mail-Adresse wird als Antwortadresse für die Lieferantenbenachrichtigung verwendet.

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

Detaillierte Informationen zum Thema

- Lieferantenbenachrichtigung prüfen auf Seite 80
- Lieferantenbenachrichtigung deaktivieren auf Seite 80
- Einrichten des E-Mail-Benachrichtigungssystems auf Seite 81

Lieferantenbenachrichtigung prüfen

HINWEIS: Die Lieferantenbenachrichtigung können Sie im Launchpad nur auf einer One Identity Manager-Datenbank mit der Staging-Ebene **Produktivumgebung** konfigurieren.

Um zu prüfen, ob die Lieferantenbenachrichtigung aktiviert ist

- Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.

  Im Bereich **Installationsübersicht** wird im Eintrag **Lieferantenbenachrichtigung konfigurieren** angezeigt, ob die Funktion aktiviert ist.

Detaillierte Informationen zum Thema

- Lieferantenbenachrichtigung aktivieren auf Seite 79
- Lieferantenbenachrichtigung deaktivieren auf Seite 80

Lieferantenbenachrichtigung deaktivieren

HINWEIS: Die Lieferantenbenachrichtigung können Sie im Launchpad nur auf einer One Identity Manager-Datenbank mit der Staging-Ebene **Produktivumgebung** konfigurieren.

Um die Lieferantenbenachrichtigung zu deaktivieren

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Installationsübersicht** den Eintrag **Lieferantenbenachrichtigung konfigurieren** und klicken Sie **Starten**.

   Der Designer wird gestartet und der Konfigurationsparametereditor geöffnet.
3. Deaktivieren Sie den Konfigurationsparameter **Common | MailNotification | VendorNotification**.

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

Verwandte Themen

- Lieferantenbenachrichtigung aktivieren auf Seite 79
- Lieferantenbenachrichtigung prüfen auf Seite 80

Einrichten des E-Mail-Benachrichtigungssystems

Der One Identity Manager versendet bei verschiedenen Aktionen im System E-Mail-Benachrichtigungen. So werden innerhalb der Bestellprozesse verschiedene Benachrichtigungen an die Besteller und Entscheider versendet. Ebenso werden Benachrichtigungen über Attestierungsvorgänge versendet oder Berichte per E-Mail zugestellt. Innerhalb der Prozessverarbeitung werden bei erfolgreicher oder fehlerhafter Ausführung einer Aktion E-Mail Benachrichtigungen versendet.

Zusätzlich zu den vordefinierten Benachrichtungsprozessen können Sie kundenspezifische Benachrichtigungen implementieren.

Um das Benachrichtigungssystems nutzen

1. Wählen Sie im Launchpad im Bereich **Konfigurieren** den Eintrag **E-Mail-Versand konfigurieren**.
2. Klicken Sie **Starten**.
3. Auf der Startseite des E-Mail-Konfigurationsassistenten klicken Sie **Weiter**.
4. Auf der Seite **Verbindung zum SMTP-Server** konfigurieren Sie die Verbindung zum SMTP-Server, der für den E-Mail-Versand genutzt werden soll.
    - Um die Angaben zum Benutzerkonto zu testen, klicken Sie **Verbindung prüfen**.
    - **SMTP-Server**: SMTP-Server, der zum Versenden von E-Mail-Benachrichtigungen genutzt wird. Ist kein Server angegeben, wird **localhost** verwendet.
    - **Benutzername**: Name des Benutzerkontos zur Authentifizierung am SMTP Server.
    - **Domäne**: Domäne des Benutzerkontos zur Authentifizierung am SMTP Server.
    - **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos zur Authentifizierung am SMTP Server.
    - **Port**: Port des SMTP-Dienstes auf dem SMTP Server. Standard: **25**

- **Transportsicherheit**: Verschlüsselungsverfahren beim Versenden von E-Mail-Benachrichtigungen. Wenn keine der folgenden Optionen angegeben wird, richtet sich das Verhalten nach dem Port (Port 25: ohne Verschlüsselung; Port 465: mit SSL/TLS Verschlüsselung).

  Zulässige Werte sind:

  - **Auto**: Automatische Erkennung des Verschlüsselungsverfahrens.
  - **SSL**: Verschlüsseln der gesamten Sitzung mit SSL/TLS.
  - **STARTTLS**: Verwenden der STARTTLS-Mailserver-Erweiterung. Schaltet die TLS-Verschlüsselung nach dem Greeting und dem Lesen der Capabilities des Servers an. Die Verbindung scheitert, wenn der Server die STARTTLS-Erweiterung nicht unterstützt.
  - **STARTTLSWhenAvailable**: Verwenden der STARTTLS-Mailserver-Erweiterung, wenn verfügbar. Schaltet die TLS-Verschlüsselung nach dem Greeting und dem Lesen der Capabilities des Servers an, jedoch nur, wenn dieser die STARTTLS-Erweiterung unterstützt.
  - **None**: Keine Sicherheit der Transportschicht. Alle Daten werden als Klartext gesendet.
- **Selbstsignierte Zertifikate akzeptieren**: Gibt an, ob selbstsignierte Zertifikate für TLS-Verbindungen akzeptiert werden.
- **Servernamenkonflikte in Zertifikaten zulassen**: Gibt an, ob nicht passende Servernamen bei den Zertifikaten für TLS-Verbindungen zulässig sind.

5. Auf der Seite **SMTP-Jobserver festlegen** wählen Sie mindestens einen Jobserver, der die Funktion **SMTP-Server** übernimmt.
6. Auf der Seite **E-Mail-Einstellungen** können Sie die Standard-E-Mail-Adresse von Absender und Empfänger sowie das Layout der E-Mails definieren.

   - **Adresse des Empfängers**: Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen.
   - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.

     Syntax:

     ```
     sender@example.com
     ```

     Beispiel:

     ```
     NoReply@company.com
     ```

     Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

     Beispiel:

     ```
     One Identity <NoReply@company.com>
     ```

- **Sprachkultur**: Standardsprachkultur, in der E-Mail-Benachrichtigungen versendet werden, wenn für einen Empfänger keine Sprachkultur ermittelt werden kann.
- **Sprache**: Standardsprache, in der E-Mail-Benachrichtigungen versendet werden.
- **Schriftart**: Standardschriftart für E-Mail-Benachrichtigungen.
- **Schriftgröße**: Standardschriftgröße für E-Mail-Benachrichtigungen.
- **Unterschrift**: Unterschrift unter die Grußformel.
- **Unternehmen**: Name des Unternehmens.
- **Link**: Link auf die Unternehmenswebseite.
- **Link-Darstellung**: Anzeigetext für den Link zur Unternehmenswebseite.

7. Auf der Seite **Datensicherheit** können Sie die Einstellungen für die Datensicherheit konfigurieren.

   - **Fingerabdruck des Zertifikats**: SHA1-Fingerabdruck des zur Signierung zu verwendenden Zertifikats. Dieses kann im Zertifikatsspeicher des Computers oder des Benutzers liegen.

     HINWEIS: Stellen Sie sicher, dass der private Schlüssel im Zertifikat als exportierbar markiert ist.

     Wenn Sie eine digitale Signatur nutzen wollen, aktivieren Sie **Fingerabdruck des Zertifikats** und geben Sie den Fingerabdruck an.
   - **Verschlüsselung**: Gibt an, ob E-Mails verschlüsselte werden sollen. Wenn Sie die Funktion aktivieren, werden die dafür benötigten Einstellungen angezeigt.
   - **Domänen-Controller**: Domänen-Controller der abzufragenden Domäne, der verwendet werden soll.
   - **Domäne**: Definierter Name der abzufragenden Domäne.
   - **Benutzerkonto**: Benutzerkonto, mit dem das Active Directory abgefragt wird.
   - **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos.

8. Auf der Seite **E-Mail-Benachrichtigungen über Bestellungen** nehmen Sie allgemeine Einstellungen für E-Mail-Benachrichtigungen über Bestellungen vor. Des Weiteren definieren Sie, ob die Funktion **Entscheidung per E-Mail** für Bestellungen genutzt werden kann. Wenn Sie die Funktion aktivieren, werden die dafür benötigten Einstellungen angezeigt.

   - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.

     Syntax:

     `sender@example.com`

     Beispiel:

     `NoReply@company.com`

Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

Beispiel:

```
One Identity <NoReply@company.com>
```

- **Tägliche Benachrichtigungen über offene Entscheidungen**: Gibt an, ob Entscheider nur einmal täglich eine E-Mail-Benachrichtigung erhalten sollen, wenn für sie Bestellungen zur Entscheidung vorliegen.

  Wenn die Funktion deaktiviert ist, erhalten Entscheider sofort eine E-Mail-Benachrichtigung, sobald eine Bestellung entschieden werden kann. Um die Anzahl der E-Mail-Benachrichtigungen zu verringern, aktivieren Sie die Funktion. Die Funktion **Entscheidung per E-Mail** kann dann nicht genutzt werden.

  > TIPP: Um eine andere als die Standardmailvorlage für diese Benachrichtigungen zu nutzen, ändern Sie den Wert des Konfigurationsparameters **QER | ITShop | MailTemplateIdents | RequestApproverByCollection** im Designer.

- **IT Shop Entscheidungen per E-Mail**: Gibt an, ob für die Entscheidung von Bestellungen auch die Funktion **Entscheidung per E-Mail** genutzt werden kann. Wenn Sie die Funktion aktivieren, bearbeiten Sie die dafür benötigten Einstellungen. Die Funktion **Tägliche Benachrichtigungen über offene Entscheidungen** kann dann nicht genutzt werden.
- **Benutzername**: Name des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Domäne**: Domäne des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Webservice URL**:
- **Postfach**: Microsoft Exchange Postfach, an das Entscheidungen per E-Mail gesendet werden.
- **Löschverhalten**: Gibt die Art und Weise an, wie E-Mails im Posteingang gelöscht werden sollen.
- **Anwendungs-ID**: Exchange Online Anwendungs-ID für die Authentifizierung über OAuth 2.0. Wenn der Wert nicht gesetzt ist, werden die Authentifizierungsmethoden **Basic** oder **NTML** verwendet.

9. Auf der Seite **E-Mail-Benachrichtigungen über Attestierungen** nehmen Sie allgemeine Einstellungen für E-Mail-Benachrichtigungen über Attestierungen vor. Des Weiteren definieren Sie, ob die Funktion **Entscheidung per E-Mail** für Attestierungen genutzt werden kann. Wenn Sie die Funktion aktivieren, werden die dafür benötigten Einstellungen angezeigt.

- **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.

  Syntax:

  ```
  sender@example.com
  ```

  Beispiel:

  ```
  NoReply@company.com
  ```

  Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

  Beispiel:

  ```
  One Identity <NoReply@company.com>
  ```

- **Tägliche Benachrichtigungen über offene Entscheidungen**: Gibt an, ob Attestierer nur einmal täglich eine E-Mail-Benachrichtigung erhalten sollen, wenn für sie Attestierungsvorgänge zur Entscheidung vorliegen.

  Wenn die Funktion deaktiviert ist, erhalten Attestierer sofort eine E-Mail-Benachrichtigung, sobald ein Attestierungsvorgang entschieden werden kann. Um die Anzahl der E-Mail-Benachrichtigungen zu verringern, aktivieren Sie die Funktion. Die Funktion **Entscheidung per E-Mail** kann dann nicht genutzt werden.

  > TIPP: Um eine andere als die Standardmailvorlage für diese Benachrichtigungen zu nutzen, ändern Sie den Wert des Konfigurationsparameters **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** im Designer.

- **Attestierung per E-Mail**: Gibt an, ob für Attestierungen auch die Funktion **Entscheidung per E-Mail** genutzt werden kann. Wenn Sie die Funktion aktivieren, bearbeiten Sie die dafür benötigten Einstellungen. Die Funktion **Tägliche Benachrichtigungen über offene Entscheidungen** kann dann nicht genutzt werden.
- **Benutzername**: Name des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Domäne**: Domäne des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Webservice URL**:
- **Postfach**: Microsoft Exchange Postfach, an das Entscheidungen per E-Mail gesendet werden.
- **Löschverhalten**: Gibt die Art und Weise an, wie E-Mails im Posteingang gelöscht werden sollen.

- **Anwendungs-ID**: Exchange Online Anwendungs-ID für die Authentifizierung über OAuth 2.0. Wenn der Wert nicht gesetzt ist, werden die Authentifizierungsmethoden **Basic** oder **NTML** verwendet.

10. Auf der Seite **Berichtsabonnements** können Sie die Standardeinstellungen für Berichtsabonnements ändern.

    - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen über Berichtsabonnements. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.

      Syntax:

      `sender@example.com`

      Beispiel:

      `NoReply@company.com`

      Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

      Beispiel:

      `One Identity <NoReply@company.com>`

    - **Standard-Berichtsvorlage**: Standardbericht, der als Vorlage zur Erstellung von einfachen Listenberichten verwendet wird.
    - **Zentrale Berichtsablage**: Gibt an, ob abonnierte Berichte in einem Ablageverzeichnis gespeichert werden sollen. Wenn Sie die Funktion aktivieren, bearbeiten Sie die dafür benötigten Einstellungen.
    - **Ablageverzeichnis für Berichte**: Pfad für die Ablage der abonnierten Berichte. Syntax: `\\<Server>\<Share>`
    - **Aufbewahrungszeitraum (Tage)**: Maximale Verweildauer (in Tagen), während der ein abonnierter Bericht im Ablageverzeichnis verfügbar ist. Nach Ablauf dieser Frist werden Berichte gelöscht.

11. Auf der Seite **E-Mail-Benachrichtigungen über Aktionen im Zielsystem** können Sie eine E-Mail-Adresse für Benachrichtigungen über Aktionen im Zielsystem hinterlegen. Das können Fehler- oder Erfolgsmeldungen über Änderungen im Zielsystem sein.

    - **<Zielsystemtyp>**: Gibt an, ob E-Mail-Benachrichtigungen mit Fehler- oder Erfolgsmeldungen über Änderungen in Zielsystemen mit diesem Typ versendet werden. Wenn Sie die Funktion aktivieren, erfassen Sie die E-Mail-Adresse, an welche die Benachrichtigungen gesendet werden sollen.

12. Auf der letzten Seite des E-Mail-Konfigurationsassistenten klicken Sie **Fertig**.

Zusätzlich können für die verschiedenen Benachrichtigungsprozesse weitere Konfigurationsparameter erforderlich sein. Diese aktivieren Sie im Designer. Einige Konfigurationsparameter stehen erst zur Verfügung wenn die Module vorhanden sind.

Tabelle 18: Weitere Konfigurationsparameter für die Mailbenachrichtigung

Konfigurationsparameter	Bedeutung
Common | InternationalEMail	Gibt an, ob internationale Domänennamen beziehungsweise Unicode-Zeichen in E-Mail-Adressen unterstützt werden. WICHTIG: Der Mailserver muss diese Funktion ebenfalls unterstützen. Gegebenenfalls müssen Sie das Skript `VID_IsSMTPAddress` überschreiben.
Common | MailNotification | Encrypt | EncryptionCertificateScript	Der Konfigurationsparameter enthält das Skript, welches eine Liste von Verschlüsselungszertifikaten liefert (Standard: `QBM_GetCertificates`).
Common | MailNotification | NotifyAboutWaitingJobs	Gibt an, ob eine Benachrichtigung gesendet werden soll, wenn Prozessschritte eines bestimmten Ausführungszustandes in der Jobqueue sind.
Common | MailNotification | SMTPUseDefaultCredentials	Gibt an, welche Anmeldeinformationen für die Authentifizierung am SMTP Server verwendet werden. Ist der Konfigurationsparameter aktiviert, werden zur Authentifizierung am SMTP Server die Anmeldeinformationen des One Identity Manager Service verwendet. Ist der Konfigurationsparameter nicht aktiviert, werden die in den Konfigurationsparametern **Common | MailNotification | SMTPDomain** und **Common | MailNotification | SMTPAccount** oder **Common | MailNotification | SMTPPassword** hinterlegten Anmeldeinformationen verwendet. (Standard)
Common | MailNotification | VendorNotification	E-Mail Adresse der Kontaktperson ihres Unternehmens. Die E-Mail-Adresse wird als Antwortadresse für die Lieferantenbenachrichtigung verwendet. Ist der Konfigurationsparameter aktiviert, erzeugt der One Identity Manager einmal im Monat eine Liste der Systemeinstellungen und sendet die Liste an One Identity. Diese Liste enthält keine personenbezogenen Daten. Sie können die aktuellsten Systeminformationen jederzeit aus dem Menü **Hilfe > Info** überprüfen. Die Liste wird von unserem Kunden-Support-Team proaktiv überprüft, welches nach wesentlichen Änderungen schaut um mögliche Probleme zu identifizieren bevor sie sich auf Ihrem System verwirklichen. Die Listen können von unseren F&E-Mitarbeitern für die Analyse, Diagnose und Replikation zu Testzwecken verwendet werden. Diese Informationen behalten Gültigkeit,

Konfigurationsparameter	Bedeutung
	solange Ihr Unternehmen weiterhin Pflegeleistungen für dieses Produkt bezieht.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Standard-E-Mail-Adresse zum Versenden von Warnmails.

Verwandte Themen

- Einrichten von Jobservern auf Seite 90
- Meldung: Enter email address in configuration parameter auf Seite 193
- Konfigurationsparameter für das E-Mail-Benachrichtigungssystem auf Seite 211

Installieren und Konfigurieren des One Identity Manager Service

Die Verarbeitung der definierten Prozesse erfolgt über den One Identity Manager Service. Zur Prozessverarbeitung muss der Dienst auf den Servern des One Identity Manager-Netzwerkes installiert sein. Die Server müssen in der One Identity Manager-Datenbank als Jobserver bekannt gegeben werden.

Die Einrichtung eines Jobservers umfasst folgende Schritte:

- Erstellen Sie einen Eintrags für den Jobserver in der One Identity Manager-Datenbank.
- Legen Sie die Maschinenrollen und Serverfunktionen für den Jobserver fest.

  Abhängig von den gewählten Maschinenrollen werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden. Die Serverfunktion definiert die Funktion eines Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.
- Installieren Sie den One Identity Manager Service.
- Konfigurieren Sie den One Identity Manager Service.
- Starten Sie den One Identity Manager Service.

Ausführliche Informationen zur Arbeitsweise des One Identity Manager Service finden Sie im *One Identity Manager Konfigurationshandbuch*.

HINWEIS: Auf Linux Betriebssystemen wird die Verwendung des Docker-Images oneidentity/oneim-job empfohlen.

Verwandte Themen

- One Identity Manager Docker-Images auf Seite 52
- Einrichten von Jobservern auf Seite 90
- One Identity Manager Service mit dem Server Installer installieren auf Seite 91
- Protokolldatei des One Identity Manager Service anzeigen auf Seite 94
- Benutzerkonto oder der Startart des One Identity Manager Service ändern auf Seite 96

- Der One Identity Manager Service im Cluster auf Seite 97
- Aktualisieren des One Identity Manager auf Seite 110
- Maschinenrollen und Installationspakete auf Seite 209

Einrichten von Jobservern

Jeder Jobserver innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt diesem Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert.

- Für jede Queue muss ein Jobserver in der One Identity Manager-Datenbank bekannt sein.
- Die Queue-Bezeichnung tragen Sie in die Konfigurationsdatei des One Identity Manager Service ein.

Jobserver können Sie über verschiedene Wege einrichten:

- Bei der initialen Schemainstallation mit dem Configuration Wizard richten Sie bereits einen Jobserver mit den Serverfunktionen **SQL Ausführungsserver** und **Aktualisierungsserver** ein. Mit dem Configuration Wizard konfigurieren Sie den Dienst und installieren den Dienst auf einem Server.
- Weitere Jobserver richten Sie mit dem Programm Server Installer ein.

  Mit dem Server Installer erstellen Sie den Jobserver mit seinen Maschinenrollen und Serverfunktionen in der Datenbank. Mit dem Server Installer konfigurieren Sie den Dienst und installieren den Dienst auf einem Server.
- Jobserver können Sie im Designer erstellen.

  Im Designer können Sie einen Jobserver mit die Maschinenrollen und Serverfunktionen erstellen, den Dienst auf dem Server konfigurieren und remote installieren. Ausführliche Informationen finden Sie *One Identity Manager Konfigurationshandbuch*.
- Alternativ können Sie die Dienstkomponenten mit dem Installationsassistenten auf dem Server installieren. Anschließend konfigurieren Sie den Dienst mit dem Programm Job Service Configuration. Ausführliche Informationen zur Konfiguration des One Identity Manager Service finden Sie *One Identity Manager Konfigurationshandbuch*.
- Wenn der Konfigurationsparameter **Common | Jobservice | AutoCreateServerFromQueues** aktiviert ist, werden bei Anfragen des One Identity Manager Service für unbekannte Queues neue Jobserver in der Datenbank erzeugt. Die Informationen zu Maschinenrollen und Serverfunktionen werden in die Datenbank übertragen.

HINWEIS: Wenn Sie nachträglich in der Datenbank Serverfunktionen für einen Jobserver ändern, beispielsweise mit dem Designer, wird geprüft, ob die benötigten Komponenten auf dem Server installiert sind und gegebenenfalls der Server aktualisiert. Dazu muss die

automatische Softwareaktualisierung aktiv sein.

Verwandte Themen

- One Identity Manager-Datenbank installieren und konfigurieren auf Seite 61
- One Identity Manager Service mit dem Server Installer installieren auf Seite 91
- One Identity Manager-Komponenten installieren auf Seite 53
- Inbetriebnahme der automatischen Softwareaktualisierung auf Seite 107

One Identity Manager Service mit dem Server Installer installieren

WICHTIG: Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, beachten Sie die Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77.

Um einen Jobserver einzurichten, führen Sie folgende Schritte aus.

1. Erstellen Sie einen Jobserver und installieren und konfigurieren Sie den One Identity Manager Service.

   Um den One Identity Manager Service zu installieren, nutzen Sie das Programm Server Installer. Das Programm führt folgende Schritte aus:

   - Erstellen eines Jobservers.
   - Festlegen der Maschinenrollen und Serverfunktionen für den Jobserver.
   - Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
   - Konfigurieren des One Identity Manager Service.
   - Starten des One Identity Manager Service.

   Mit dem Server Installer können Sie den One Identity Manager Service lokal oder remote installieren.

   Für die Remote-Installation des One Identity Manager Service stellen Sie eine administrative Arbeitstation bereit, auf der die One Identity Manager-Komponenten installiert sind. Für eine lokale Installation stellen Sie sicher, dass die One Identity Manager-Komponenten auf dem Server installiert sind. Ausführliche Informationen zur Installation der One Identity Manager-Komponenten finden Sie im *One Identity Manager Installationshandbuch*.

2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.

3. Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Erfassen der Verbindungsinformationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um den One Identity Manager Service auf einem Server zu installieren und zu konfigurieren

1. Starten Sie das Programm Server Installer.

   HINWEIS: Für eine Remote-Installation starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation. Für eine lokale Installation starten Sie das Programm auf dem Server.

2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.

   Für die Verbindung zur Datenbank können Sie eine Verbindung über den Anwendungsserver oder die direkte Verbindung verwenden.

3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.

   a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

      - ODER -

      Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.

   b. Bearbeiten Sie folgende Informationen für den Jobserver.

      - **Server**: Bezeichnung des Jobservers.
      - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder Jobserver innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
      - **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

        Syntax:

        ```
        <Name des Servers>.<Vollqualifizierter Domänenname>
        ```

   HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.

4. Auf der Seite **Maschinenrollen** legen Sie fest, welche Rolle der Jobserver im One Identity Manager übernimmt. Abhängig von der gewählten Maschinenrolle werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden.

5. Auf der Seite **Serverfunktionen** legen Sie die Funktion des Servers in der One Identity Manager-Umgebung fest. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

   Die Serverfunktionen sind abhängig von den gewählten Maschinenrollen bereits ausgewählt. Sie können die Serverfunktionen hier weiter einschränken.

6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

   HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.

   Für eine direkte Verbindung zu Datenbank:

   a. Wählen Sie in der Modulliste **Prozessabholung > sqlprovider**.
   b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   d. Klicken Sie **OK**.

   Für eine Verbindung zum Anwendungsserver:

   a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.
   b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.
   c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.
   d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.
   f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
   g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
   h. Klicken Sie **OK**.

7. Zur Konfiguration der Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.

10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

      Um die Installation lokal auszuführen, wählen Sie in der Auswahlliste den Eintrag **<lokale Installation>**.
    - **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

    Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen.

    Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.
11. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
12. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

    HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.

Verwandte Themen

- Minimale Systemanforderungen für Jobserver auf Seite 41
- Benutzer für den One Identity Manager auf Seite 46
- Benutzerkonto oder der Startart des One Identity Manager Service ändern auf Seite 96
- Maschinenrollen und Installationspakete auf Seite 209

Protokolldatei des One Identity Manager Service anzeigen

Die Anzeige der One Identity Manager Service Protokolldatei ist über ein Browserfrontend möglich.

Der Aufruf der Protokolldatei erfolgt mit der entsprechenden URL:

http://<Servername>:<Portnummer>

Standard ist der Port 1880.

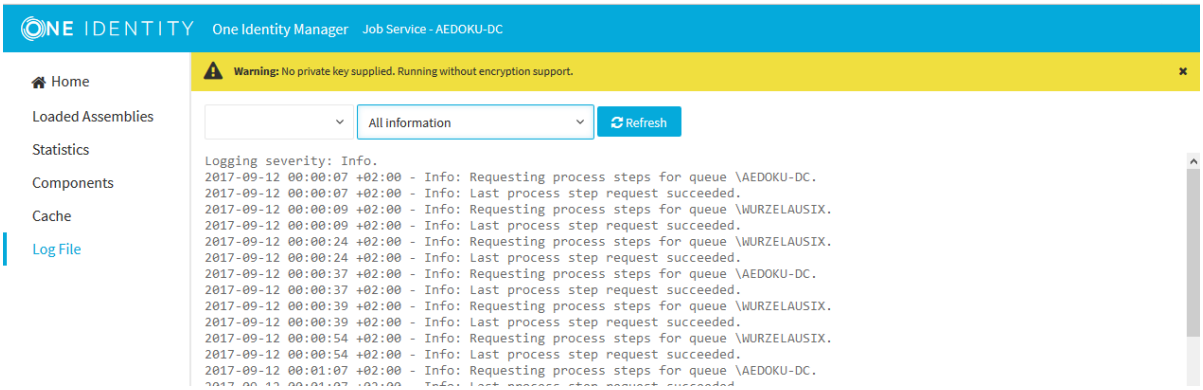
Abhängig vom konfigurierten Authentifizierungsverfahren für die Anzeige der Protokolldatei werden verschiedene Anmeldedaten erwartet.

Um die Protokolldatei des One Identity Manager Service im Job Queue Info zu öffnen

1. Starten Sie das Programm Job Queue Info.
2. Wählen Sie in der Ansicht **Serverstatus** den Jobserver und wählen Sie das Kontextmenü **Im Browser öffnen**.

   Es wird für einen Jobserver der HTTP Server des One Identity Manager Service angesprochen und die verschiedenen Dienste des One Identity Manager Service werden angezeigt.
3. Um den Inhalt der Protokolldatei anzuzeigen, wählen Sie in der Navigationsansicht **Log File**.

Abbildung 3: Protokolldatei des One Identity Manager Service



Die auf der Webseite anzuzeigenden Meldungen können interaktiv gefiltert werden. Dazu gibt es auf der Webseite eine Auswahlliste. Dabei können nur Texte angezeigt werden, die auch in der Protokolldatei vorhanden sind. Steht beispielsweise der Informationsgrad auf **Warning** können auch bei entsprechender Filterwahl keine Meldungen mit dem Informationsgrad **Info** eingeblendet werden.

Zur besseren Übersichtlichkeit werden die Protokollausgaben farbig gekennzeichnet.

Tabelle 19: Farbcode in der Protokolldatei

Farbe	Bedeutung
Grün	Die Verarbeitung war erfolgreich.
Gelb	Bei der Verarbeitung wurden Warnung ausgegeben.
Rot	Bei der Verarbeitung sind schwerwiegende Fehler aufgetreten.

TIPP: Um die Farbinformationen der Protokolldatei für den Mailversand zu erhalten, speichern Sie die komplette Webseite.

Ausführliche Informationen zur Konfiguration der Anzeige der One Identity Manager Service Protokolldatei finden Sie im *One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge*.

Benutzerkonto oder der Startart des One Identity Manager Service ändern

HINWEIS:

- In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.
- Wenn Sie das Benutzerkonto des One Identity Manager Service ändern, müssen Sie die Konfigurationsdatei des Dienstes erneut im Installationsverzeichnis des Dienstes ablegen.
- Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, beachten Sie die Hinweise zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank auf Seite 77.

Um die Anmeldedaten und die Startart des Dienstes anzupassen

1. Öffnen Sie die Dienstverwaltung des Servers und wählen Sie in der Liste der Dienste den Eintrag **One Identity Manager Service**.
2. Öffnen Sie über den Kontextmenüeintrag **Eigenschaften** die Eigenschaften des Dienstes.
3. Ändern Sie auf dem Tabreiter **Allgemein** den Starttyp, sofern erforderlich.

   Es wird der Starttyp **Automatisch** empfohlen.
4. Ändern Sie auf dem Tabreiter **Anmelden** das Benutzerkonto, unter dem der Dienst läuft.
5. Klicken Sie auf **Übernehmen**.
6. Schließen Sie die Eigenschaften des Dienstes über **OK**.
7. Starten Sie den Dienst über den Kontextmenüeintrag **Starten**.

   Kann der One Identity Manager Service nicht gestartet werden, wird eine entsprechende Meldung in das Ereignisprotokoll des Servers geschrieben.

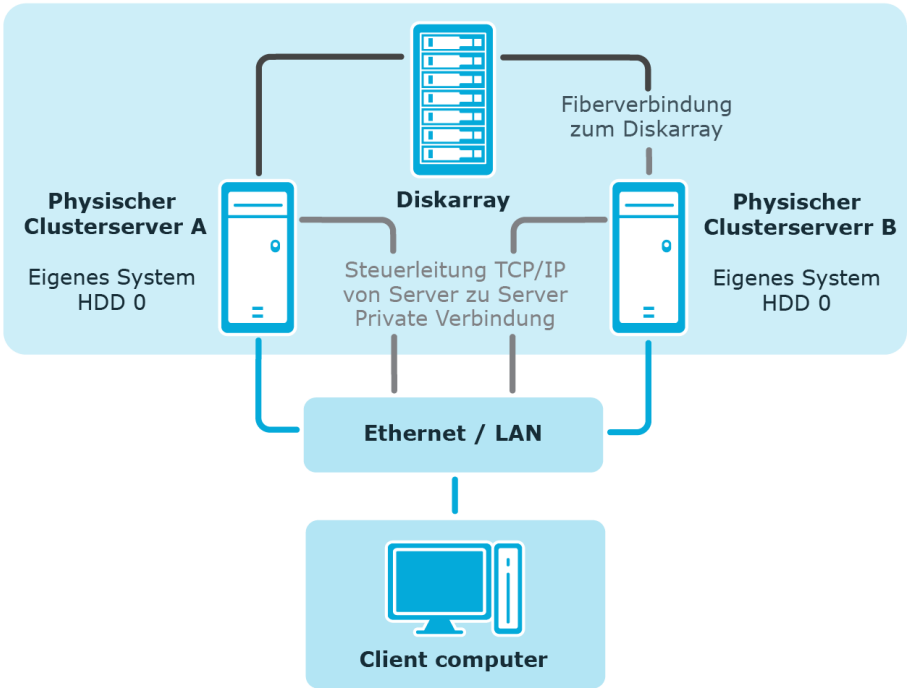
Verwandte Themen

- Minimale Systemanforderungen für Jobserver auf Seite 41
- Benutzer für den One Identity Manager auf Seite 46

Der One Identity Manager Service im Cluster

Sinn einer Clusterlösung ist die Hochverfügbarkeit eines Systems. Es wird angestrebt, beim Versagen einer Hardwarekomponente oder einer Softwarekomponente, den Systemausfall auf einige Sekunden zu beschränken. Mit der Installation einer Windows-Clusterlösung (nur mit Enterprise–Servern möglich) kann dies erreicht werden. Die folgende Grafik zeigt ein Beispiel für eine derartige Lösung.

Abbildung 4: Beispiel einer Clusterlösung



Dieser Cluster besteht aus 2 physikalischen Maschinen "Server A" und "Server B", die ein gemeinsames Diskarray nutzen und jeweils über eine eigene Systemfestplatte verfügen. Jeder Server ist mit einem Windows Betriebssystem ausgestattet. Beide Server sind identisch installiert, so dass im Falle eines Ausfalls der eine Server die Arbeit des anderen Servers übernehmen kann.

Alle redundanten Systemkomponenten werden durch den Cluster-Manager verwaltet. Nach außen wird der Cluster als ein einzelner, virtueller Server "Server C" angesprochen. Hierbei wird der zugreifende Dienst oder Benutzer automatisch zu dem physikalischen Server verbunden, der momentan die Arbeit im Cluster ausführt.

Tritt ein Versagen auf einem der physikalischen Server ein, so übernimmt automatisch der redundante Server im Cluster. Ansprechpartner bleibt weiter der virtuelle Server, nur der physikalische Server, der die Arbeit ausführt, wechselt.

Detaillierte Informationen zum Thema

- Registrieren des One Identity Manager Service im Cluster auf Seite 98
- Installieren und Konfigurieren des One Identity Manager Service im Cluster auf Seite 98

Registrieren des One Identity Manager Service im Cluster

Mit der Registrierung unterliegt der One Identity Manager Service der Clusterbehandlung für Ausfallsicherheit und Lastverteilung. Der Dienst wird auf dem virtuellen Server installiert, den der Cluster simuliert. Alle rechnerbezogenen Operationen und Informationen des Dienstes gehen, für den Dienst transparent, gegen den virtuellen Server statt gegen den realen aktuellen Rechner (Cluster Knoten). Das gilt auch für die Clients, die den Dienst über den Servernamen kontaktieren, beispielsweise via RPC (ORPC, DCOM), TCP/IP (Winsock, Named Pipes), HTTP.

Da der Dienst sich im Kontext des virtuellen Servers befindet, sind die folgenden Fakten zu beachten:

- Die dienstspezifischen Einstellungen auf dem Knoten, auf dem sich der virtuelle Server befindet, werden auf alle anderen Knoten repliziert. Der Dienst hat somit immer die gleiche Konfiguration, unabhängig von dem Knoten, auf dem er aktuell gestartet ist.
- Der Dienst ist immer nur auf dem aktuellen Knoten des virtuellen Servers (der Knoten, der aktuell den virtuellen Server trägt) gestartet. Auf allen anderen Knoten ist der Dienst gestoppt.
- Der Dienst wird mit dem virtuellen Server heruntergefahren und hochgefahren. Ist der Cluster inaktiv, ist der Dienst auf allen Knoten gestoppt.
- Die Dienste auf den Knoten werden automatisch vor der Registrierung durch das Programm in den erforderlichen Zustand (**Manual** und **Stopped**) gebracht.

Verwandte Themen

- Der One Identity Manager Service im Cluster auf Seite 97
- Installieren und Konfigurieren des One Identity Manager Service im Cluster auf Seite 98

Installieren und Konfigurieren des One Identity Manager Service im Cluster

Die Installation und Konfiguration der Serverkomponenten vom One Identity Manager-Installationsmedium führen Sie auf allen physikalischen Knoten eines Clusters durch.

HINWEIS: Bei der Konfiguration der JobServiceDestination muss der Parameter **Queue** den Namen des virtuellen Servers enthalten.

Nach dem Speichern der Konfiguration kopieren Sie die Konfigurationsdatei in das Installationsverzeichnis des One Identity Manager Service auf allen physikalischen Knoten. Dabei dürfen Sie auch den Namen der Konfigurationsdatei nicht ändern.

HINWEIS: Die Konfiguration des One Identity Manager Service ist nicht Bestandteil einer Clusterressource. Somit hält jeder Knoten seine eigene Konfiguration. Achten Sie aus diesem Grund darauf, dass die Konfigurationsdateien auf allen physikalischen Knoten des Clusters konsistent sind. Ist dies nicht der Fall, kann nicht für die korrekte Funktionsweise nach einem Wechsel des Clusterknotens garantiert werden.

Einrichten einer Clusterressource für den One Identity Manager Service

Richten Sie im Programm Cluster Administrator eine neue Clusterressource für den One Identity Manager Service ein und bringen diese online. Die Vorgehensweise entnehmen Sie der Microsoft Technet unter http://technet.microsoft.com/en-us/library/cc787285(WS.10).aspx. Beachten Sie bei der Erstellung der Clusterressource Folgendes:

- Wählen Sie **Generic Service** als Ressourcentyp.
- Wählen Sie mindestens folgende Abhängigkeiten des One Identity Manager Service.
    - Cluster IP-Address
    - Cluster Name
    - Quorum; zum Beispiel Disk: D
- Geben Sie keine weiteren Registrierungsschlüssel an.

HINWEIS: Nach der Einrichtung des One Identity Manager Service in einem Clusterverbund ist es ratsam, ein Failover zu simulieren, damit eventuell vorhandene Probleme am Cluster nicht erst im produktiven Betrieb zu Tage treten.

Auslagern der Protokolldatei des One Identity Manager Service in ein Shared Volume

- Richten Sie im Programm Cluster Administrator eine neue Clusterressource ein und bringen Sie diese online. Beachten Sie bei der Erstellung der Clusterressource Folgendes.
    - Wählen Sie **File Share** als Ressourcentyp.
    - Wählen Sie mindestens die folgende Abhängigkeit aus:

      One IdentityOne Identity Manager Service
- Passen Sie in der Konfigurationsdatei des One Identity Manager Service die Verzeichnisangabe im Parameter **Protokolldatei** (`OutPutFile`) des Logwriters an.
- Kopieren Sie die Konfigurationsdatei nach der Änderung auf alle physischen Knoten des Clusters in das Installationsverzeichnis des One Identity Manager Service.

Verwandte Themen

- Der One Identity Manager Service im Cluster auf Seite 97
- Registrieren des One Identity Manager Service im Cluster auf Seite 98

6

Automatisches Aktualisieren des One Identity Manager

Aufgrund der räumlichen Verteilung der Server und Arbeitsstationen gestaltet sich vor allem das manuelle lokale Installieren und Aktualisieren von Software als problematisch. Um einen erträglichen Arbeitsaufwand der Netzwerkadministratoren zu gewährleisten, wurde für den One Identity Manager ein Verfahren zur automatischen Aktualisierung des One Identity Manager entwickelt. Neben der Aktualisierung bekannter Dateien einer One Identity Manager-Installation können neue, kundenspezifische Dateien auf einfache Weise in das Verfahren aufgenommen werden und somit über die Mechanismen der automatischen Softwareaktualisierung an die Arbeitsstationen und Server eines One Identity Manager-Netzwerkes verteilt werden.

Detaillierte Informationen zum Thema

- Grundlagen zur automatischen Softwareaktualisierung auf Seite 101
- Inbetriebnahme der automatischen Softwareaktualisierung auf Seite 107
- Automatische Softwareaktualisierung deaktivieren auf Seite 108

Grundlagen zur automatischen Softwareaktualisierung

Alle Dateien einer One Identity Manager-Installation sind mit Namen und ihrem Binärcode in der One Identity Manager-Datenbank in der Tabelle `QBMFileRevision` abgelegt. Für jede Datei die Dateigröße und ein Hashwert zur Dateierkennung hinterlegt. Zusätzlich ist für jede Datei ist in der Tabelle `QBMFileHasDeployTarget` die Zugehörigkeit zu den Maschinenrollen und Installationspaketen erfasst.

Die benötigten Dateien werden beim Einspielen eines Hotfixes, eines Service Packs oder einer Versionsänderung in die One Identity Manager-Datenbank eingefügt und aktualisiert.

In der Datenbank wird ein Semaphor `Softwarerevision` gepflegt. Beim Hinzufügen, Ändern oder Löschen einer Datei in der Datenbank wird der Semaphorwert durch den DBQueue Prozessor neu berechnet. Im Installationsverzeichnis aller One Identity Manager-

Installationen liegt eine Datei `Softwarerevision.viv`. Diese Datei ist im Dateisystem mit den Berechtigungen **nur lesen** und **nicht sichtbar** gekennzeichnet und wird damit vom Betriebssystem normalerweise nicht angezeigt.

Die Datei `Softwarerevision.viv` enthält die folgenden Informationen:

- den Revisionsstand der Installation

  Der Revisionsstand wird aus dem Wert des Semaphors **Softwarerevision** in der Datenbank ermittelt.
- den Startzeitpunkt der letzten Änderung

Ab One Identity Manager Version 8.0 wird die Datei `Update.zip` in der Tabelle `QBMFileRevision` abgelegt. Die Datei spielt eine zentrale Rolle in der automatischen Aktualisierung. Das Zip-Archiv enthält alle Dateien, die auf den Clients oder Servern für die Produktaktualisierung notwendig sind. Das Zip-Archiv ist nicht Bestandteil der One Identity Manager Installationsdaten, sondern wird nach der Aktualisierung der Datenbank vom Configuration Wizard und auch vom Software Loader neu erstellt.

Bestandteil des Zip-Archivs sind folgende Dateien

- `Update.exe`
- `VI.Base.dll`
- `NLog.dll`
- `Newtonsoft.Json.dll`
- `InstallManager.Msi.dll`
- `InstallManager.Core.dll`

Das Zip-Archiv wird mit allen Dateien aus den Installationsdaten erweitert, die dem Namensfilter `*.Update.dll` entsprechen. Damit ist es möglich, dass verschiedene Module weitere Funktionalitäten zur automatischen Aktualisierung beisteuern.

Zusätzlich befindet sich im Installationsverzeichnis aller One Identity Manager-Installationen eine Datei `InstallState.config`. Diese Datei enthält die Informationen über die installierten Maschinenrollen, Installationspakete und Dateien.

Durch den Vergleich der Semaphorwerte aus der Datenbank und der Datei `Softwarerevision.viv` wird festgestellt, ob eine Softwareaktualisierung notwendig ist. Unterscheiden sich die Semaphorwerte, wird anhand der `InstallState.config` ermittelt, welche Maschinenrollen für den Computer oder den Server definiert sind. Für jede Datei, die zu einer Maschinenrolle gehört, wird geprüft, ob diese Datei in der Datenbank bekannt ist.

Gibt es die Datei in der Datenbank, wird geprüft:

- Hat sich die Dateigröße geändert?

  Ist dies der Fall, wird die Datei in die Liste der zu aktualisierenden Dateien aufgenommen.
- Hat sich der Hashwert geändert?

  Ist dies der Fall, wird die Datei in die Liste der zu aktualisierenden Dateien aufgenommen.

Neue Dateien, die durch das Einspielen eines Hotfixes, eines Service Packs, einer Versionsänderung oder durch Einspielen einer kundenspezifischen Datei in die One Identity Manager-Datenbank geladen wurden, werden ebenfalls in die Liste aufgenommen. Alle in der Liste aufgeführten Dateien werden aktualisiert.

Alle Aktionen werden in der Datei `update.log` protokolliert. Nach Abschluss der Aktualisierung wird der aktuelle Semaphorwert aus der Datenbank in die Datei `Softwarerevision.viv` übernommen.

Verwandte Themen

- Automatische Aktualisierung der One Identity Manager-Werkzeuge auf Seite 103
- Automatische Aktualisierung des One Identity Manager Service auf Seite 105
- Automatische Aktualisierung von Webanwendungen auf Seite 106
- Inbetriebnahme der automatischen Softwareaktualisierung auf Seite 107
- Automatische Softwareaktualisierung deaktivieren auf Seite 108

Automatische Aktualisierung der One Identity Manager-Werkzeuge

Beim Start eines Programms stellt die `VI.DB.dll` die Verbindung zur Datenbank her und führt den Semaphortest aus. Wird die Datei `SoftwareRevision.viv` nicht gefunden, so wird eine neue Datei angelegt.

Ist im Installationsverzeichnis des One Identity Manager keine Schreibberechtigung vorhanden, wird eine Fehlermeldung ausgegeben und die Softwareaktualisierung fortgesetzt.

Das Aktualisierungsprogramm (`Update.exe`) erwartet bei aktivierter Benutzerkontensteuerung die Angabe einer administrativen Anmeldung, sofern der angemeldete Benutzer keine administrativen Berechtigungen auf das Installationsverzeichnis besitzt (zum Beispiel `%ProgramFiles%`). Erfolgt die Installation in ein Verzeichnis, dass nicht über die Benutzerkontensteuerung verwaltet wird, entfällt diese Abfrage. Anschließend wird der Aktualisierungsprozess gestartet.

Die Anwendung lädt die Datei `Update.zip` aus der Datenbank oder holt diese Datei vom Anwendungsserver. Die Datei wird in einem temporären Verzeichnis entpackt.

Im ersten Schritt teilt die `Update.exe` der Hauptanwendung mit, ob sie eine Aktualisierung durchführen kann. Abhängig von der Konfiguration kann der Anwender jetzt eventuell noch die automatische Aktualisierung abbrechen.

Um den Start weiterer Anwendungen während der Aktualisierungsphase zu unterbinden, wird im Installationsverzeichnis eine Datei `Update.Lock` erzeugt. Das auslösende Programm und das Aktualisierungsprogramm (`Update.exe`) schreiben ihre Prozess-ID in die Datei. Nach erfolgreichem Abschluss der Aktualisierung wird die `Update.Lock`-Datei aus dem Installationsverzeichnis gelöscht. Das Programm wird anschließend neu gestartet. Um sicherzustellen, dass nach einem unerwarteten Programmabbruch in der Aktualisierungsphase, die automatische Aktualisierung bei Neustart einer Anwendung

erneut startet, wird eine `Update.Lock`-Datei, die älter als zwei Stunden ist, ignoriert. Ist bei Neustart einer Anwendung keiner der Prozesse, deren ID's in der `Update.Lock`-Datei stehen, auf der Arbeitsstation vorhanden, so wird die `Update.Lock`-Datei ebenfalls ignoriert und die Aktualisierung erneut gestartet.

Vor der eigentlichen Aktualisierung werden die Vorbereitungsschritte aus den `*.Update.dlls` aufgerufen, die die Installation auf die Aktualisierung vorbereiten. Ein Vorbereitungsschritt kann beispielsweise die Umbenennung einer Maschinenrolle sein.

Für die eigentliche Aktualisierung ermittelt die `Update.exe` alle notwendigen Dateien und speichert diese in einem temporären Verzeichnis. Die Kommunikation mit dem System erfolgt dabei über die zu aktualisierende Clientanwendung, da nur diese die erforderlichen Berechtigungen zum Kontaktieren der Datenbank oder des Anwendungsservers besitzt. Sind alle erforderlichen Dateien übertragen, so übernimmt die `Update.exe` die Steuerung und beginnt mit dem Dateiaustausch. An dieser Stelle wird der Anwender aufgefordert, die noch geöffnete Anwendung zu beenden, wenn sie den Aktualisierungsprozess verhindert. Gleichzeitig erfolgt eine Anforderung von Administrationsberechtigungen per Benutzerkontensteuerung, falls diese nötig sind.

Bei diesem Aktualisierungsvorgang werden nicht nur die Dateien ausgetauscht, sondern es erfolgt auch die Ausführung von weiteren Migrationsschritten aus den `*.Update.dlls`. Die Funktionalität in diesen Migrationsschritten ist nicht beschränkt. Typische Beispiele sind Anpassungen in der Registrierungsdatenbank oder in den Konfigurationsdateien und das Entfernen von veralteten Programminformationen auf den Rechnern. Diese Migrationsschritte werden ausgeführt, nachdem die Dateien ausgetauscht wurden.

Konnten alle Aktualisierungsschritte erfolgreich ausgeführt werden, so erstellt die `Update.exe` eine neue `SoftwareRevision.viv` und startet die Clientanwendung neu. Danach beendet sich die `Update.exe` und entfernt selbst das temporäre Arbeitsverzeichnis. Die Softwareaktualisierung ist damit abgeschlossen.

Im laufenden Betrieb wird durch die `VI.DB.dll` zyklisch der Semaphortest ausgeführt. Wird eine Datei zum Austausch erkannt, so wird der Aktualisierungsprozess gestartet.

Verwandte Themen

- Eingreifen des Benutzers in die automatische Aktualisierung der One Identity Manager-Werkzeuge auf Seite 104

Eingreifen des Benutzers in die automatische Aktualisierung der One Identity Manager-Werkzeuge

Wird die Aktualisierung der One Identity Manager-Komponenten auf einer Arbeitsstation erkannt, erfolgt der Hinweis alle geöffneten Programme zu schließen. Nachdem der Benutzer alle Programme geschlossen hat, wird die Aktualisierung ausgeführt.

Ob die Benutzer der One Identity Manager-Werkzeuge entscheiden können, wann die Aktualisierung ihrer Arbeitsstationen erfolgt, wird über den Konfigurationsparameter **Common | AutoUpdate | AllowOutOfTimeApps** gesteuert.

- Ist der Konfigurationsparameter nicht aktiviert, hat ein Benutzer keine Möglichkeit in die Aktualisierung einzugreifen. Die Aktualisierung wird sofort ausgeführt.
- Ist der Konfigurationsparameter aktiviert, wird dem angemeldeten Benutzer ein Meldungsfenster angezeigt. Der Benutzer kann entscheiden, ob die Aktualisierung der One Identity Manager-Werkzeuge auf seiner Arbeitsstation sofort oder zu einem späteren Zeitpunkt ausgeführt wird.

  HINWEIS: Lehnt der Benutzer die sofortige Aktualisierung ab, so kann er weiterarbeiten. Die Aktualisierung kann dann mit dem nächsten Start des Programms durchgeführt werden.

Automatische Aktualisierung des One Identity Manager Service

Die automatische Softwareaktualisierung ist das Standardverfahren zur Aktualisierung des One Identity Manager Service auf den Servern. Im Aktualisierungsverfahren wurde jedoch berücksichtigt, dass es unter Umständen unumgänglich ist, einzelne Server von der automatischen Aktualisierung auszuschließen und manuell zu aktualisieren.

Der One Identity Manager Service liefert bei jeder Anfrage nach Prozessschritten seinen aktuellen Stand des Semaphors **Softwarerevision** zurück. Sollte dieser Wert von dem in der Datenbank gefundenen Wert abweichen, so wird der Jobserver in der Datenbank als "in Aktualisierung befindlich" gekennzeichnet und es werden keine normalen Prozessschritte für diesen Jobserver mehr geliefert.

Abhängig vom eingestellten Verfahren im Konfigurationsparameter **Common | Autoupdate | ServiceUpdateType** wird die Aktualisierung der Jobserver durchgeführt.

Es wird zunächst der Startzeitpunkt der letzten Änderung aus der Datei `SoftwareRevision.viv` ermittelt. Es wird eine Liste aller Dateien mit der Zusatzinformation, ob es sich um eine neue Datei handelt, zusammengestellt. Diese Liste wird auf dem zu aktualisierenden Jobserver ausgewertet und eine Liste erstellt, welche der Dateien zu aktualisieren sind.

Der Dienst erhält vom Server dafür einen `AutoUpdate`-Prozess. Dieser Prozess lädt die Datei `Update.zip` und der Aktualisierungsvorgang beginnt.

Sollte die Aktualisierung mit dem neuen Verfahren nicht abgeschlossen werden können, weil beispielsweise keine direkte Verbindung zur Datenbank oder einem Anwendungsserver besteht, werden die Dateien über Prozessschritte in der Jobqueue übertragen (Fallback). In diesem Fall können eventuell vorhandene Aktualisierungsschritte aus den Modulbibliotheken nicht ausgeführt werden.

Wurde mindestens eine Datei auf dem Jobserver ausgetauscht, erfolgt ein Neustart des One Identity Manager Service. Nach Abschluss der Aktualisierung wird die Kennzeichnung des Jobservers in der Datenbank wieder zurückgesetzt.

Automatische Aktualisierung von Webanwendungen

Grundsätzlich unterstützen die Webanwendungen die automatische Softwareaktualisierung. Für die einzelnen Webanwendungen können jedoch eigene Konfigurationseinstellungen erforderlich sein, um an der automatischen Softwareaktualisierung teilzunehmen.

Für die automatische Aktualisierung sind folgende Berechtigungen erforderlich:

- Das Benutzerkonto für die Aktualisierung benötigt die Berechtigung zum Schreiben auf das Anwendungsverzeichnis.
- Das Benutzerkonto für die Aktualisierung benötigt die lokale Sicherheitsrichtlinie **Anmelden als Stapelverarbeitungsauftrag**.
- Das Benutzerkonto, unter dem der Anwendungspool läuft, benötigt die lokalen Sicherheitsrichtlinien **Ersetzen eines Tokens auf Prozessebene** und **Anpassen von Speicherkontingenten für einen Prozess**.

Die Aktualisierung einer Webanwendung erfordert einen Neustart der Webanwendung. Der Neustart der Webanwendung erfolgt durch den Webserver automatisch, wenn die Webanwendung eine definierte Zeitspanne keine Benutzeraktivität aufweist. Dies kann einige Zeit dauern oder durch ununterbrochene Benutzeranfragen verhindert werden. Einige Webanwendungen bieten die Möglichkeit den Neustart manuell auszuführen.

HINWEIS: Um das Web Portal automatisch zu aktualisieren, verbinden Sie sich in einem Browser auf den Runtime Monitor http://<servername>/<application>/monitor und starten Sie die Aktualisierung der Webanwendung.

Wird die Aktualisierung der Webanwendung erkannt, werden neue Dateien aus der Datenbank in vorläufige Verzeichnisse auf den Server kopiert.

Die Anwendung lädt zusätzlich die Datei `Update.zip` aus der Datenbank oder holt diese Datei vom Anwendungsserver. Die Datei wird in einem temporären Verzeichnis entpackt.

Die `Update.exe` wird gestartet und wartet bis der Webanwendungsprozess herunter gefahren wird. Die `Update.exe` kopiert die Dateien aus dem vorläufigen Verzeichnis in das Verzeichnis der Webanwendung.

Verwandte Themen

- Anwendungsserver aktualisieren auf Seite 141
- Automatische Aktualisierung für das Web Designer Web Portal konfigurieren auf Seite 164
- Manager Webanwendung aktualisieren auf Seite 175

Inbetriebnahme der automatischen Softwareaktualisierung

Folgende Berechtigungen werden für die automatische Softwareaktualisierung benötigt:

- Für die automatische Aktualisierung der One Identity Manager-Werkzeuge werden volle Zugriffsberechtigungen auf das One Identity Manager-Installationsverzeichnis empfohlen.
- Für die automatische Aktualisierung des One Identity Manager Service benötigt das Benutzerkonto des Dienstes Vollzugriff auf das One Identity Manager-Installationsverzeichnis.

Um die automatische Softwareaktualisierung einzusetzen

1. Stellen Sie sicher, dass ein Aktualisierungsserver eingerichtet ist. Dieser Server sorgt für die automatische Aktualisierung der weiteren Server.
    - Der Server muss als Jobserver mit der Serverfunktion **Aktualisierungsserver** in der Datenbank eingetragen sein.
    - Auf dem Server muss ein One Identity Manager Service mit direktem Zugriff auf die Datenbank installiert und konfiguriert sein.
2. Prüfen Sie im Designer den Konfigurationsparameter **Common | Autoupdate**.
    - Ist der Konfigurationsparameter aktiviert (Standard), dann werden Dateien des One Identity Manager, die nicht dem erforderlichen Revisionsstand entsprechen, automatisch aktualisiert.
    - Ist der Konfigurationsparameter deaktiviert, erfolgt keine automatische Softwareaktualisierung.
3. Legen Sie über den Konfigurationsparameter **Common | AutoUpdate | AllowOutOfTimeApps** fest, ob die Benutzer der One Identity Manager-Werkzeuge entscheiden können, wann die Aktualisierung ihrer Arbeitsstation erfolgt.
    - Ist der Konfigurationsparameter aktiviert, wird den Benutzern der One Identity Manager-Werkzeuge ein Meldungsfenster angezeigt, mit dem sie festlegen, ob die Aktualisierung sofort oder zu einem späteren Zeitpunkt erfolgen soll.
    - Ist der Konfigurationsparameter nicht aktiviert, werden die One Identity Manager-Werkzeuge sofort aktualisiert.
4. Legen Sie im Konfigurationsparameter **Common | Autoupdate | ServiceUpdateType** fest, welches Verfahren für die Aktualisierung des One Identity Manager Service genutzt wird.

Tabelle 20: Verfahren laut Konfigurationsparameter Common | Autoupdate | ServiceUpdateType

Verfahren	Bedeutung
Queue	Es wird ein Prozess in die Jobqueue eingestellt, über den die Dateien verteilt werden.
DB	Die Dateien werden direkt aus der Datenbank geladen. Dieses Verfahren setzen Sie ein, wenn alle Jobserver eine direkte Datenbankverbindung haben.
Auto	Alle Kopfserver werden direkt aus der Datenbank befüllt. Für alle Blattserver wird ein Prozess in die Jobqueue eingestellt. Für dieses Verfahren müssen die Kopfserver eine direkte Datenbankverbindung haben.

5. Für die Aktualisierung der Webanwendungen können eigene Konfigurationseinstellungen notwendig sein. Prüfen Sie diese Konfigurationseinstellungen.

Verwandte Themen

- Grundlagen zur automatischen Softwareaktualisierung auf Seite 101
- Automatische Softwareaktualisierung deaktivieren auf Seite 108

Automatische Softwareaktualisierung deaktivieren

HINWEIS: Ist der Konfigurationsparameter **Common | Autoupdate** deaktiviert, erfolgt systemweit keine automatische Softwareaktualisierung.

Unter Umständen ist es erforderlich einzelne Arbeitstationen, Server oder Webanwendungen von der automatischen Aktualisierung auszuschließen.

Automatische Aktualisierung einer Arbeitsstation deaktivieren

Um auf einer Arbeitsstation die automatische Aktualisierung lokal zu deaktivieren, setzen Sie den Registrierungsschlüssel `HKEY_CURRENT_USER\Software\One Identity\One Identity Manager\Global\Settings\AutoUpdateEnabled` auf den Wert **false**.

Damit wird die automatische Aktualisierung auf dieser Arbeitsstation komplett deaktiviert.

Automatische Aktualisierung eines Jobservers deaktivieren

Die automatische Aktualisierung von Jobservern konfigurieren Sie im Jobservereintrag.

Um einzelne Jobserver von der automatischen Aktualisierung auszuschließen

1. Wählen Sie im Designer die Kategorie **Basisdaten > Installationen > Jobserver**.
2. Wählen Sie in der Jobserverübersicht den Jobserver zur Bearbeitung aus.
3. Aktivieren Sie auf dem Tabreiter **Eigenschaften** die Option **kein automatisches Softwareupdate**.
4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Automatische Aktualisierung des Web Designer Web Portals deaktivieren

Die Aktualisierung eines Web Designer Web Portal können Sie in der Datenbank deaktivieren.

Um die automatische Aktualisierung des Web Designer Web Portals zu deaktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Webserver Einstellungen**.
2. Wählen Sie in der Listenansicht den Eintrag für das Web Designer Web Portal.
3. Ändern Sie auf dem Tabreiter **Eigenschaften** den Wert für die Spalte **Auto-Update-Status** auf den Wert **inaktiv**.
4. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Automatische Aktualisierung eines Anwendungsservers deaktivieren

Die automatische Aktualisierung konfigurieren Sie in der Datei `web.config` des Anwendungsservers. Weitere Informationen finden Sie unter Anwendungsserver aktualisieren auf Seite 141.

7

Aktualisieren des One Identity Manager

Die Aktualisierung des One Identity Manager beinhaltet die Aktualisierung der One Identity Manager-Datenbank und die Aktualisierung der vorhandenen Installationen auf den Arbeitsstationen und Servern eines One Identity Manager-Netzwerkes.

Zur Aktualisierung des One Identity Manager werden einzelne Hotfixes und Service Packs zu einer Hauptversion oder vollständige Versionsänderungen zur Verfügung gestellt.

- Hotfix

  Ein Hotfix enthält einzelne Korrekturen an der Standardkonfiguration der eingesetzten Hauptversion jedoch keine Erweiterungen der Funktionalität. Ein Hotfix kann Patches für gelöste Probleme in Synchronisationsprojekten bereitstellen.

- Service Pack

  Ein Service Pack enthält geringfügige Erweiterungen der Funktionalität sowie alle Änderungen seit der letzten Hauptversion, die bereits in den Hotfixes enthalten waren. Ein Service Pack kann Patches mit neuen Funktionen für Synchronisationsprojekte bereitstellen.

- Versionsänderung

  Eine Versionsänderung ist verbunden mit signifikanten Erweiterungen der Funktionalität und umfasst eine Komplettänderung der Installation. Eine Versionsänderung kann Meilensteine für die Aktualisierung von Synchronisationsprojekten bereitstellen. Meilensteine fassen alle Patches für gelöste Probleme und notwendige Patches für neue Funktionen der Vorversion zusammen.

Detaillierte Informationen zum Thema

- Ablauf der Aktualisierung bei Freigabe einer neuen One Identity Manager Version auf Seite 111
- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- One Identity Manager-Komponenten mit dem Installationsassistenten aktualisieren auf Seite 114
- Aktualisieren der One Identity Manager-Datenbank auf Seite 117

Ablauf der Aktualisierung bei Freigabe einer neuen One Identity Manager Version

HINWEIS: Lesen Sie die Versionshinweise für eventuell abweichende oder zusätzliche Schritte zur Aktualisierung des One Identity Manager.

Um den One Identity Manager auf eine neue Version zu aktualisieren

1. Führen Sie im Designer alle Konsistenzprüfungen im Bereich **Datenbank** aus.
    a. Starten Sie den Konsistenzeditor im Designer über den Menüeintrag **Datenbank > Datenkonsistenz überprüfen**.
    b. Klicken Sie im Dialog **Testeinstellungen** das Symbol .
    c. Aktivieren Sie alle Tests im Bereich **Datenbank** und klicken Sie **OK**.
    d. Starten Sie die Prüfung über das Menü **Konsistenztest > Starten**.

    Alle Datenbanktests müssen erfolgreich sein. Korrigieren Sie die Fehler. Einige Konsistenzprüfungen bieten Reparaturmethoden zur Fehlerkorrektur an.
2. Aktualisieren Sie die administrative Arbeitsstation, auf welcher die Schemaaktualisierung der One Identity Manager-Datenbank gestartet wird.
    a. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
    b. Wechseln Sie auf den Tabreiter **Installation**. Wählen Sie die Edition, die Sie installiert haben.
    c. Klicken Sie **Installieren**.

    Der Installationsassistent wird gestartet.
    d. Folgen Sie den Installationsanweisungen.

    WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
3. Beenden Sie den One Identity Manager Service auf dem Aktualisierungsserver.
4. Erstellen Sie eine Sicherung der One Identity Manager-Datenbank.
5. Prüfen Sie, ob der Kompatibilitätsgrad der Datenbank auf den Wert **150** eingestellt ist und passen Sie die Wert bei Bedarf an.
6. Führen Sie die Schemaaktualisierung der One Identity Manager-Datenbank aus.
    - Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation.

Verwenden Sie für die Aktualisierung des One Identity Manager Schemas mit dem Configuration Wizard einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.

- Verwenden Sie denselben Benutzer, den Sie auch für die initiale Schemainstallation verwendet haben.
- Haben Sie bei der Schemainstallation einen administrativen Benutzer erstellt, dann verwenden Sie diesen Benutzer.
- Haben Sie zur Schemainstallation einen Benutzer mit Windows-Authentifizierung gewählt, dann müssen Sie diesen Benutzer zur Aktualisierung verwenden.

> HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 9.1.3 auf das abgestufte Berechtigungskonzept wechseln möchten, verwenden Sie den Installationsbenutzer laut Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29.
>
> Passen Sie nach der Aktualisierung des One Identity Manager die Verbindungsparameter an. Die betrifft beispielsweise die Verbindungsinformationen für die Datenbank (`DialogDatabase`), den One Identity Manager Service, die Anwendungsserver, die Administrations- und Konfigurationswerkzeuge, die Webanwendungen und die Webservices sowie die Verbindungsinformationen in Synchronisationsprojekten.
>
> Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

7. Aktualisieren Sie den One Identity Manager Service auf dem Aktualisierungsserver.
   a. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
   b. Wechseln Sie auf den Tabreiter **Installation**. Wählen Sie die Edition, die Sie installiert haben.
   c. Klicken Sie **Installieren**.

      Der Installationsassistent wird gestartet.
   d. Folgen Sie den Installationsanweisungen.

      > WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
8. Prüfen Sie die Anmeldeinformationen des One Identity Manager Service. Geben Sie das zu verwendende Dienstkonto an.
9. Starten Sie den One Identity Manager Service auf dem Aktualisierungsserver.
10. Aktualisieren Sie weitere Installationen auf Arbeitsstationen und Servern.

Für die Aktualisierung vorhandener Installationen können Sie das Verfahren der automatischen Softwareaktualisierung einsetzen.

HINWEIS: Unter Umständen kann es erforderlich sein, die weiteren Arbeitsstationen und Jobserver manuell zu aktualisieren. Dies ist beispielsweise erforderlich, wenn sich mit einem One Identity Manager-Versionswechsel signifikante Neuerungen ergeben, die den Einsatz der automatischen Softwareaktualisierung nicht zulassen.

Um Synchronisationsprojekte auf eine neue Version zu aktualisieren

Beim Aktualisieren des One Identity Manager werden gegebenenfalls Änderungen an den Systemkonnektoren oder der Synchronization Engine bereitgestellt. Damit alle bereits eingerichteten Zielsystemsynchronisationen weiterhin fehlerfrei ausgeführt werden, müssen diese Änderungen auf bestehende Synchronisationsprojekte angewendet werden. Dafür werden Patches bereitgestellt.

HINWEIS: Einige Patches werden automatisch angewendet. Dafür wird ein Prozess in die Jobqueue eingestellt, der alle vorhandenen Synchronisationsprojekte migriert. Damit der Prozess ausgeführt werden kann, muss der One Identity Manager Service auf dem Datenbankserver und auf allen Synchronisationsservern gestartet sein.

- Prüfen Sie, ob der Prozess `DPR_Migrate_Shell` erfolgreich ausgeführt wurde.

  Wenn ein Patch nicht angewendet werden konnte, beispielsweise weil das Zielsystem nicht erreichbar war, können Sie diesen Patch nachträglich manuell anwenden.

Detaillierte Informationen zum Anwenden von Patches finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Um einen Anwendungsserver auf eine neue Version zu aktualisieren

- Nach der Schemaaktualisierung der One Identity Manager-Datenbank startet der Anwendungsserver die automatische Aktualisierung.
- Um die Aktualisierung manuell zu starten, öffnen Sie die Statusseite des Anwendungsservers im Browser und klicken Sie im Menü des angemeldeten Benutzers **Update immediately**.

Um das Web Designer Web Portal auf eine neue Version zu aktualisieren

HINWEIS: Stellen Sie sicher, dass der Anwendungsserver aktualisiert ist, bevor Sie das Web Portal aktualisieren.

- Um dasWeb Designer Web Portal automatisch zu aktualisieren, verbinden Sie sich in einem Browser auf den Runtime Monitor http://<servername>/<application>/monitor und starten Sie die Aktualisierung der Webanwendung.
- Um das Web Designer Web Portal manuell zu aktualisieren, deinstallieren Sie die bestehende Web Designer Web Portal Installation und installieren Sie das Web Designer Web Portal neu.

Um einen API Server auf eine neue Version zu aktualisieren

- Nach der Schemaaktualisierung der One Identity Manager-Datenbank starten Sie den API Server neu. Der API Server wird automatisch aktualisiert.

Um das Web Portal für Betriebsunterstützung auf eine neue Version zu aktualisieren

- (von Version 8.1.x) Nach der Aktualisierung des API Servers ist das Web Portal für Betriebsunterstützung ebenfalls aktuell.
- (von Version 8.0.x)
  1. Deinstallieren Sie das Web Portal für Betriebsunterstützung.
  2. Installieren Sie einen API Server. Ausführliche Anweisungen finden Sie im *One Identity Manager Installationshandbuch*.

Um die Manager Webanwendung auf eine neue Version zu aktualisieren

1. Deinstallieren Sie die Manager Webanwendung.
2. Installieren Sie die Manager Webanwendung neu.
3. Damit die Manager Webanwendung automatisch aktualisiert werden kann, benötigt der Standardbenutzer des Internet Information Services Bearbeitungsberechtigungen auf das Installationsverzeichnis der Manager Webanwendung. Prüfen Sie, ob die entsprechenden Berechtigungen vorhanden sind.

Detaillierte Informationen zum Thema

- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- One Identity Manager-Komponenten mit dem Installationsassistenten aktualisieren auf Seite 114
- Aktualisieren der One Identity Manager-Datenbank auf Seite 117
- Installieren und Aktualisieren eines Anwendungsservers auf Seite 135
- Installieren des API Servers auf Seite 145
- Installieren, Konfigurieren und Warten des Web Designer Web Portals auf Seite 152
- Installieren und Aktualisieren der Manager Webanwendung auf Seite 171

One Identity Manager-Komponenten mit dem Installationsassistenten aktualisieren

HINWEIS: Für die Aktualisierung der Arbeitsstationen und Server können Sie das Verfahren der automatischen Softwareaktualisierung einsetzen. Weitere Informationen

finden Sie unter Automatisches Aktualisieren des One Identity Manager auf Seite 101.

Unter Umständen kann es erforderlich sein, Arbeitsstationen und Server manuell mit dem Installationsassistenten zu aktualisieren. Dies ist beispielsweise erforderlich, wenn sich mit einem One Identity Manager-Versionswechsel signifikante Neuerungen ergeben, die den Einsatz der automatischen Softwareaktualisierung nicht zulassen.

HINWEIS: Bei einem Versionswechsel oder bei der Installation weiterer Module in eine bestehende One Identity Manager-Installation aktualisieren Sie die Arbeitsstation, auf der die Schemainstallation der One Identity Manager-Datenbank gestartet wird, mit dem Installationsassistenten.

Um eine Arbeitsstation mit dem Installationsassistenten zu aktualisieren

1. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
2. Wechseln Sie auf den Tabreiter **Installation**. Wählen Sie die Edition, die Sie installiert haben.

   HINWEIS: Um eine One Identity Manager Active Directory Edition zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager Active Directory Edition**.
3. Klicken Sie **Installieren**.

   Der Installationsassistent wird gestartet.
4. Auf der Startseite wählen Sie die Sprache für den Installationsassistenten und klicken Sie **Weiter**.
5. Bestätigen Sie die Lizenzbedingungen.
6. Auf der Seite **Einstellungen für die Installation** erfassen Sie folgenden Informationen.
   - **Installationsquelle**: Wählen Sie das Verzeichnis mit den Installationsdateien.
   - **Installationsverzeichnis**: Wählen Sie das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.

     HINWEIS: Um weitere Konfigurationseinstellungen vorzunehmen, klicken Sie auf die Pfeil Schaltfläche neben dem Eingabefeld. Hier können Sie festlegen, ob die Installation auf einem 64 Bit- Betriebssystem oder auf einem 32 Bit-Betriebssystem erfolgt.

     Für eine Standardinstallation nehmen Sie keine weiteren Konfigurationseinstellungen vor.
   - **Installationsmodule mit der Datenbank auswählen**: Um die Installationsinformationen über die vorhandene One Identity Manager-Datenbank zu laden sind, aktivieren Sie die Option.

     HINWEIS: Für Installation der Arbeitsstation, auf der Sie die Installation des One Identity Manager Schemas starten, lassen Sie die Option deaktiviert.

- **Weitere Module zur gewählten Edition hinzufügen**: Um zusätzliche One Identity Manager Module zur gewählten Edition hinzuzufügen, aktivieren Sie die Option.

7. Auf der Seite **Datenbank verbinden** erfassen Sie die Informationen zur Datenbankverbindung.

   HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen** aktiviert haben.

   - Wählen Sie im Bereich **Datenbankverbindung auswählen** die Verbindung.

     - ODER -

   - Klicken Sie auf **Neue Verbindung erstellen**, wählen Sie den Systemtyp **SQL Server** und erfassen Sie die Verbindungsdaten.
     - **Server**: Datenbankserver.
     - (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
     - **Nutzer**: SQL Server Anmeldename des Benutzer.
     - **Kennwort**: Kennwort für die SQL Server Anmeldung des Benutzer.
     - **Datenbank**: Wählen Sie die Datenbank.

8. Auf der Seite **Modulauswahl** wählen Sie die zusätzlich zu installierenden Module.

   HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Option **Weitere Module zur gewählten Edition hinzufügen** aktiviert haben.

9. Auf der Seite **Maschinenrolle zuordnen** legen Sie die Maschinenrollen fest.

   HINWEIS: Die zur vorhandenen Installation passenden Maschinenrollen sind aktiviert.

10. Auf der Seite **WebView2 installieren** werden Sie aufgefordert, Microsoft Edge WebView2 zu installieren. Die Benutzeroberfläche einiger One Identity Manager-Komponenten benötigt Microsoft Edge WebView2, um bestimmte Inhalte darstellen zu können.

    HINWEIS: Diese Seite wird nur angezeigt, wenn Sie One Identity Manager-Komponenten installieren möchten, die WebView2 erwarten und WebView2 noch nicht installiert ist.

11. Auf der letzten Seite des Installationsassistenten können Sie verschiedene Programme für die weitere Installation starten.

    - Um die Installation des One Identity Manager Schemas auszuführen, starten Sie den Configuration Wizard und folgen Sie den Anweisungen des Configuration Wizard.

HINWEIS: Führen Sie diesen Schritt nur auf der Arbeitsstation aus, auf der Sie die Installation des One Identity Manager Schemas starten.

- Um die Konfiguration des One Identity Manager Service zu erstellen, starten Sie das Programm Job Service Configuration.

  HINWEIS: Führen Sie diesen Schritt nur auf Servern aus, auf denen Sie den One Identity Manager Service installiert haben.

12. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.
13. Schließen Sie das Autorun Programm.

Um den One Identity Manager Service mit dem Installationsassistenten zu aktualisieren

1. Öffnen Sie die Dienstverwaltung des Servers und beenden Sie den One Identity Manager Service.
2. Aktualisieren Sie die One Identity Manager-Komponenten mit dem Installationsassistenten.

   WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
3. Prüfen Sie die Anmeldeinformationen des One Identity Manager Service. Geben Sie das zu verwendende Dienstkonto an.
4. Starten Sie den One Identity Manager Service in der Dienstverwaltung.

Verwandte Themen

- Maschinenrollen und Installationspakete auf Seite 209

Aktualisieren der One Identity Manager-Datenbank

Im One Identity Manager ist eine automatische Versionsverwaltung integriert, die einen konsistenten Stand der Bestandteile des One Identity Manager untereinander als auch zur Datenbank sichert. Werden Programmerweiterungen implementiert, die die Struktur verändern, beispielsweise Tabellenerweiterungen, ist eine Aktualisierung der Datenbank erforderlich.

Die Aktualisierung der Datenbank ist dann notwendig, wenn Hotfixes und Service Packs zur eingesetzten One Identity Manager-Version oder vollständige Versionsänderungen verfügbar sind. Des Weiteren ist es erforderlich, dass kundenspezifische Änderungen aus einer Entwicklungsdatenbank in die Testdatenbank und in die Datenbank des Produktivsystems zu übernehmen sind.

WICHTIG: Bevor Sie ein Transportpaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung.

Die Anpassung des One Identity Manager Schemas erfolgt durch das Einspielen so genannter Transportpakete. Der One Identity Manager kennt die folgenden Arten von Transportpaketen, die je nach Anforderung in die Datenbank zu importieren sind.

Tabelle 21: Transportpakete

Art des Transportpaketes	Beschreibung	Verwendetes Werkzeug
Migrationspaket	Migrationspakete werden für die initiale Schemainstallation der Datenbank, bei einem Service Pack und einer vollständigen Versionsänderung zur Verfügung gestellt. Ein Migrationspaket enthält alle benötigten Tabellen, Datentypen, Datenbankprozeduren sowie die Standardkonfiguration des One Identity Manager.	Configuration Wizard
Hotfixpaket	Hotfixpakete werden zur Verfügung gestellt, um einzelne Korrekturen an der Standardkonfiguration wie beispielsweise Bildungsregeln, Skripte, Prozesse oder Dateien in die Datenbank einzuspielen. Mehrere Hotfixpakete werden zu einem kumulativen Hotfixpaket zusammengefasst. HINWEIS: Enthält ein Hotfixpaket nur geänderte Dateien, laden Sie diese Dateien mit dem Programm Software Loader in die Datenbank.	Database Transporter Software Loader
Kundenkonfigurationspaket	Ein Kundenkonfigurationspaket dient zum Austausch kundenspezifischer Änderungen zwischen Entwicklungsdatenbank, Testdatenbank und Datenbank des Produktivsystems. Diese Transportpakete werden vom Kunden erstellt und in die Datenbanken eingespielt.	Database Transporter

HINWEIS: Sollen zusätzlich zu einem Hotfixpaket weitere kundenspezifische Konfigurationsanpassungen in eine One Identity Manager-Datenbank übernommen werden, können Sie dafür mit dem Database Transporter ein kumulatives Transportpaket erstellen und dieses Transportpaket in die Zieldatenbank importieren.

Verwandte Themen

- One Identity Manager-Datenbank mit dem Configuration Wizard aktualisieren auf Seite 121
- Einspielen eines Hotfixes in die One Identity Manager-Datenbank auf Seite 126

Hinweise zur Aktualisierung der One Identity Manager-Datenbank

- Bevor Sie ein Migrationspaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung. Verwenden Sie eine Kopie der produktiven Datenbank für die Tests.
- Stellen Sie vor der Aktualisierung des One Identity Manager Schemas sicher, dass der administrative Systembenutzer, mit dem die Kompilierung der Datenbank erfolgt, ein Kennwort hat. Anderenfalls kann die Aktualisierung des Schemas nicht vollständig durchgeführt werden.
- Wenn Sie ein Service Pack oder eine vollständige Versionsänderung erhalten, verwenden Sie den Configuration Wizard zur Aktualisierung der One Identity Manager-Datenbank. Der Configuration Wizard führt die Aktualisierung des Schemas durch und überträgt den aktuellen Stand in die Versionshistorie.
- Für eine One Identity Manager-Datenbank auf einem SQL Server wird aus Performancegründen empfohlen, für die Zeit der Schemaaktualisierung die Datenbank auf das Wiederherstellungsmodell **Einfach** zu setzen.
- Starten Sie den Configuration Wizard auf einer administrativen Arbeitsstation.

  Verwenden Sie für die Aktualisierung des One Identity Manager Schemas mit dem Configuration Wizard einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.

  - Verwenden Sie denselben Benutzer, den Sie auch für die initiale Schemainstallation verwendet haben.
  - Haben Sie bei der Schemainstallation einen administrativen Benutzer erstellt, dann verwenden Sie diesen Benutzer.
  - Haben Sie zur Schemainstallation einen Benutzer mit Windows-Authentifizierung gewählt, dann müssen Sie diesen Benutzer zur Aktualisierung verwenden.

  HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 9.1.3 auf das abgestufte Berechtigungskonzept wechseln möchten, verwenden Sie den Installationsbenutzer laut Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29.

  Passen Sie nach der Aktualisierung des One Identity Manager die Verbindungsparameter an. Dies betrifft beispielsweise die Verbindungsinformationen für die Datenbank (`DialogDatabase`), den One Identity

Manager Service, die Anwendungsserver, die Administrationswerkzeuge und Konfigurationswerkzeuge, die Webanwendungen und die Webservices sowie die Verbindungsinformationen in Synchronisationsprojekten.

Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

- Für den Zeitraum der Aktualisierung wird die Datenbank in den Einzelbenutzermodus gesetzt. Beenden Sie alle bestehenden Verbindungen zur Datenbank vor dem Start der Schemaaktualisierung.
- Nach Beenden der Aktualisierung wird die Datenbank automatisch in den Mehrbenutzermodus geschaltet. Sollte dies nicht möglich sein, erhalten Sie eine Meldung, über die Sie die Datenbank manuell in den Mehrbenutzermodus schalten können.
- Bei Einsatz einer Datenbankspiegelung kann es zu Problemen bei der Aktivierung des Einzelbenutzermodus kommen.
- Während der Aktualisierung werden Berechnungsaufträge in die Datenbank eingestellt. Diese werden durch den DBQueue Prozessor verarbeitet. Abhängig von Datenumfang und Systemperformance kann die Verarbeitung der Berechnungsaufträge einige Zeit dauern.

  Dies ist insbesondere der Fall, wenn Sie große Mengen historisierter Daten, wie beispielsweise Datenänderungen oder Informationen aus der Prozessverarbeitung in der One Identity Manager-Datenbank speichern.

  Stellen Sie daher vor der Aktualisierung der Datenbank sicher, dass Sie ein entsprechendes Verfahren zur Datenarchivierung konfiguriert haben. Ausführliche Informationen zur Archivierung von Daten finden Sie im *One Identity Manager Administrationshandbuch für die Datenarchivierung*.
- Damit die Kompilierung von HTML-Anwendungen erfolgreich durchgeführt werden kann, müssen Pakete aus dem NPM-Repository heruntergeladen werden. Stellen Sie daher sicher, dass die Arbeitsstation, auf der kompiliert werden soll, eine Verbindung zur Webseite registry.npmjs.org:443 herstellen kann.

  Alternativ ist es möglich, die Pakete von einem Proxy-Server herunterzuladen und manuell zur Verfügung zu stellen.

Detaillierte Informationen zum Thema

- One Identity Manager-Datenbank mit dem Configuration Wizard aktualisieren auf Seite 121
- Verarbeitung der One Identity Manager-Datenbank während der Aktualisierung mit dem Configuration Wizard auf Seite 124
- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29

One Identity Manager-Datenbank mit dem Configuration Wizard aktualisieren

WICHTIG: Bevor Sie ein Migrationspaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung. Verwenden Sie eine Kopie der produktiven Datenbank für die Tests.

HINWEIS: Starten Sie den Configuration Wizard auf einer administrativen Arbeitsstation.

Um eine Datenbank zu aktualisieren

1. Starten Sie den Configuration Wizard.
2. Auf der Startseite des Configuration Wizard wählen Sie die Option **Datenbank aktualisieren** und klicken Sie **Weiter**.
3. Auf der Seite **Datenbank auswählen** wählen Sie Datenbank und das Installationsverzeichnis.
    a. Wählen Sie im Bereich **Datenbankverbindung auswählen** die Datenbankverbindung. Verwenden Sie einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.
    b. Wählen Sie im Bereich **Installationsquellen** das Verzeichnis mit den Installationsdateien.
4. Auf der Seite **Produktbeschreibung** werden die Konfigurationsmodule und Versionsinformationen angezeigt.
    a. Wählen Sie die Module, die Sie aktualisieren möchten.
    b. Bestätigen Sie, dass von der Datenbank eine aktuelle Sicherung erstellt wurde.
    c. Bestätigen Sie, dass die Konsistenzprüfungen der Datenbank durchgeführt wurden.
    d. Sollte es erforderlich sein weitere Module auszuwählen, aktivieren Sie die Option **Weitere Module hinzufügen**.
5. Wählen Sie auf der Seite **Konfigurationsmodule auswählen** die zusätzlichen Module und bestätigen Sie die Sicherheitsmeldung.

    HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Option **Weitere Module hinzufügen** aktiviert haben.

    Wenn Sie zusätzliche Module hinzufügen, erhalten Ihre kundenspezifischen administrativen Benutzer die Berechtigungen auf diese Module.
6. Auf der Seite **Datenbanküberprüfung** werden Fehler angezeigt, die eine Verarbeitung der Datenbank verhindern. Beheben Sie die Fehler bevor Sie mit der Aktualisierung fortfahren.
7. Auf der Seite **Aktualisierungsvorgang einleiten** werden die verschiedenen Phasen zur Vorbereitung der Datenbankaktualisierung durchlaufen.

HINWEIS: Diese Seite wird nur bei Aktualisierung einer Datenbank angezeigt, die mindestens die One Identity Manager Version 8.2 hat.

Durch diese stufenweise Vorbereitung soll sichergestellt werden, dass die Benutzer über die bevorstehende Aktualisierung informiert werden und Prozesse gezielt beendet werden können.

Alternativ können Sie die Datenbankaktualisierung sofort starten. Damit werden die Vorbereitungsphasen übersprungen.

- Vorbereitungsphasen durchlaufen (Standard)
  a. Warten Sie bis der Configuration Wizard die einzelnen Phasen zur Vorbereitung der Datenbankaktualisierung abgeschlossen hat. Die Informationen zu den Phasen werden angezeigt.
  b. Klicken Sie **Weiter**.
- Datenbankaktualisierung sofort starten
  a. Klicken Sie den Link **Um die Aktualisierung sofort zu starten, klicken Sie hier**.
  b. Klicken Sie **Weiter**.

8. Falls noch Verbindungen anderer Benutzer zur Datenbank bestehen, werden diese auf der Seite **Aktive Datenbankverbindungen** angezeigt.
   - Trennen Sie die Verbindungen, damit die Verarbeitung der Datenbank gestartet werden kann.
9. Auf der Seite **Neue Anmeldung für administrative Benutzer erstellen** entscheiden Sie, welche SQL Server Anmeldung für administrative Benutzer verwendet wird.

   HINWEIS: Diese Seite wird nur bei Aktualisierung einer One Identity Manager-Datenbank von Version 8.0.x auf die Version 9.1.3 angezeigt.

   Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

   Zur Auswahl stehen:

   - **Neue SQL Server Anmeldungen für die Datenbank erstellen**: Wählen Sie diese Option, wenn Sie mit dem abgestuften Berechtigungskonzept arbeiten möchten.

     Es wird für die Datenbank eine neue, administrative Anmeldung auf dem SQL Server erstellt.

     - Erfassen Sie den Anmeldenamen, das Kennwort und die Kennwortbestätigung für die neue SQL Server Anmeldung.

     Im weiteren Verlauf werden mit dem Configuration Wizard zusätzliche SQL Server Anmeldungen für Konfigurationsbenutzer und für Endbenutzer erstellt.
   - **Aktuelle SQL Server Anmeldung für die Datenbank verwenden:** Wenn Sie diese Option wählen, werden keine zusätzlichen SQL Server Anmeldungen

für die Datenbank erstellt. In diesem Fall kann nicht mit abgestuften Berechtigungskonzepten auf SQL-Ebene gearbeitet werden.

Es wird der Benutzer verwendet, den Sie für die Verbindung zur Datenbank angegeben haben.

10. Auf der Seite **Systemadministrator-Berechtigung** erfassen Sie die Anmeldeinformationen für die Datenbankanmeldung mit Berechtigungen eines Systemadministrators.

    HINWEIS: Diese Seite wird nur angezeigt, wenn Sie mit abgestuften Berechtigungen arbeiten und Änderungen an den Berechtigungen des administrativen Benutzers vorgenommen werden müssen.

11. Auf der Seite **Verarbeitung der Datenbank** werden die Installationsschritte angezeigt. Die Installation und Konfiguration der Datenbank wird durch den Configuration Wizard automatisch durchgeführt.

    TIPP: Um detaillierte Informationen zu den Verarbeitungsschritten und zum Migrationsprotokoll zu erhalten, aktivieren Sie die Option **Erweitert**.

    a. Im Verlauf der Aktualisierung ist die Anmeldung mit einem administrativen Benutzer erforderlich.

        i. Erfassen Sie den Benutzername und Kennwort des administrativen Systembenutzers.

        ii. Klicken Sie **Anmelden**.

    b. Nach Abschluss der Verarbeitung, klicken Sie **Weiter**.

12. Auf der Seite **Neue Anmeldungen für Konfigurationsbenutzer und Endbenutzer erstellen** erfassen Sie die den Anmeldenamen, das Kennwort und die Kennwortbestätigung für die SQL Server Anmeldungen für Konfigurationsbenutzer und Endbenutzer.

    HINWEIS: Das Kennwort muss den Anforderungen der Windows Richtlinien für Kennwörter entsprechen.

    HINWEIS: Diese Seite wird nur bei Aktualisierung einer One Identity Manager-Datenbank von Version 8.0 auf die Version 9.1.3 angezeigt, wenn Sie sich auf der Seite **Neue Anmeldung für administrative Benutzer erstellen** für die abgestuften Berechtigungen entschieden haben.

13. Auf der Seite **Systeminformationen** konfigurieren Sie administrative Systembenutzer für den One Identity Manager. Erfassen Sie ein Kennwort und die Kennwortbestätigung.

    HINWEIS: Diese Seite wird nur angezeigt, wenn durch die Aktualisierung neue administrative Systembenutzer erstellt werden.

14. Auf der Seite **Lieferantenbenachrichtigung konfigurieren** können Sie die Lieferantenbenachrichtigung einrichten.

    HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Lieferantenbenachrichtigung noch nicht konfiguriert haben.

Wenn die Lieferantenbenachrichtigung aktiviert ist, erzeugt One Identity Manager einmal im Monat eine Liste der Systemeinstellungen und sendet die Liste an One Identity. Diese Liste enthält keine personenbezogenen Daten. Die Liste wird von unserem Kunden-Support-Team proaktiv überprüft, welches nach wesentlichen Änderungen schaut um mögliche Probleme zu identifizieren bevor sie sich auf Ihrem System verwirklichen. Die Listen können von unseren F&E-Mitarbeitern für die Analyse, Diagnose und Replikation zu Testzwecken verwendet werden. Diese Informationen behalten Gültigkeit, solange Ihr Unternehmen weiterhin Pflegeleistungen für dieses Produkt bezieht.

a. Um die Funktion zu nutzen, aktivieren Sie die Option **Lieferantenbenachrichtigung aktivieren** und geben Sie unter **E-Mail-Adresse für Kontakt** die E-Mail-Adresse Ihres Unternehmenskontaktes ein.

   Die E-Mail-Adresse wird als Absenderadresse für die Lieferantenbenachrichtigung verwendet.

b. Um die Funktion nicht zu nutzen, aktivieren Sie die Option **Lieferantenbenachrichtigung deaktivieren**.

15. Die Seite **Datenbankaufgaben verarbeiten** wird nur angezeigt, wenn noch Aufträge für den DBQueue Prozessor in der DBQueue bereitstehen, die während der Aktualisierung der Datenbank verarbeitet werden müssen. Nach Abschluss der Verarbeitung, klicken Sie **Weiter**.
16. Auf der letzten Seite des Configuration Wizard klicken Sie **Fertig**.

Verwandte Themen

- Hinweise zur Aktualisierung der One Identity Manager-Datenbank auf Seite 119
- Verarbeitung der One Identity Manager-Datenbank während der Aktualisierung mit dem Configuration Wizard auf Seite 124
- Lieferantenbenachrichtigung im One Identity Manager auf Seite 78
- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank auf einem SQL Server auf Seite 29
- Berechtigungen für die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 36
- Fehlermeldungen bei der Installation und der Aktualisierung der One Identity Manager-Datenbank auf Seite 190

Verarbeitung der One Identity Manager-Datenbank während der Aktualisierung mit dem Configuration Wizard

Die Aktualisierung der One Identity Manager-Datenbank wird durch den Configuration Wizard automatisch durchgeführt. Der Vorgang kann abhängig von Datenumfang und Systemperformance einige Zeit dauern.

Der Configuration Wizard führt dabei die folgenden Schritte aus:

1. Vorbereiten der Aktualisierung.

   HINWEIS: Dieser Schritt wird nur bei Aktualisierung einer Datenbank ausgeführt, die mindestens die One Identity Manager Version 8.2 hat.

   Es werden die verschiedenen Phasen zur Vorbereitung der Datenbankaktualisierung durchlaufen. Durch diese stufenweise Vorbereitung soll sichergestellt werden, dass die Benutzer über die bevorstehende Aktualisierung informiert werden und Prozesse gezielt beendet werden können. Alternativ können Sie die Datenbankaktualisierung sofort starten. Damit werden die Vorbereitungsphasen übersprungen.

   Folgende Phasen werden durchlaufen:

   - Normaler Betriebsmodus: Die Datenbank befindet sich im normalen Betriebsmodus. Der Aktualisierungsvorgang wurde noch nicht initiiert.
   - Information zur Aktualisierung: Alle Datenbanknutzer werden über die bevorstehende Aktualisierung informiert. Das System nimmt keine Prozesse mehr an. Die Vorbereitungsphase wird in der Statuszeile der Programme angezeigt.
   - Aktualisierung vorbereiten: Neue Benutzer können sich an der Datenbank nicht mehr anmelden. Alle offenen Prozesse werden noch verarbeitet. Dauert dieser Vorgang sehr lange, prüfen Sie die Jobqueue und die DBQueue auf eventuelle Prozesse. Die Vorbereitungsphase wird in der Statuszeile der Programme angezeigt.
   - Aktualisierung ausführen: Die Datenbank ist bereit für die Aktualisierung. Die Aktualisierung kann gestartet werden. Die Vorbereitungsphase wird in der Statuszeile der Programme angezeigt.

2. Aktualisieren des One Identity Manager Schemas.

   Vor der Schemaaktualisierung prüft der Configuration Wizard die Datenbank. Die Fehlermeldungen werden in einem separaten Meldungsfenster ausgegeben. Die Fehler sind manuell zu korrigieren. Erst danach kann die Schemaaktualisierung gestartet werden.

   Durch die Schemaaktualisierung werden alle benötigten Tabellen, Datentypen, Datenbankprozeduren in die Datenbank eingespielt. Beim Import eines Migrationspaketes in eine One Identity Manager-Datenbank werden die folgenden Operationen ausgeführt:

Tabelle 22: Operationen beim Import eines Migrationspaketes

Operationen	Beschreibung
Einfügen	Wird das Objekt in der Zieldatenbank nicht gefunden, so wird ein neues Objekt mit den Schlüsselwerten erzeugt.
Aktualisieren	Wird das Objekt in der Zieldatenbank gefunden, so wird das Objekt aktualisiert.
Löschen	Nicht mehr benötigte Objekte werden in der Zieldatenbank gelöscht.

Während einer Schemaaktualisierung werden Berechnungsaufträge in die Datenbank eingestellt. Diese werden durch den DBQueue Prozessor verarbeitet.

Bei einer Schemaaktualisierung mit dem Configuration Wizard werden das Migrationsdatum und der Migrationsstand in der Transporthistorie der Datenbank aufgezeichnet.

3. Kompilieren des Systems.

   Es werden die Skripte, Bildungsregeln und Prozesse in der Datenbank bekannt gegeben. Es wird das Authentifizierungsmodul **Systembenutzer** mit dem angegebenen Systembenutzer zum Kompilieren verwendet.

4. Laden der Dateien für die automatische Softwareaktualisierung.

   Um die Dateien des One Identity Manager über die Mechanismen der automatischen Softwareaktualisierung zu verteilen, werden die Dateien in die One Identity Manager-Datenbank geladen.

5. Migrieren von Synchronisationsprojekten.

   Es wird ein Prozess in die Jobqueue eingestellt, der alle vorhandenen Synchronisationsprojekte migriert. Dabei werden das One Identity Manager Schema aktualisiert und automatische Patches angewendet.

6. Finalisierung der Aktualisierung.

   Die durch die Schemaaktualisierung eingestellten Prozesse werden final verarbeitet. Abschließend wird die Datenbank in den normalen Betriebsmodus geschaltet.

Verwandte Themen

- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- Transporthistorie anzeigen und One Identity Manager Version prüfen auf Seite 188
- Fehlermeldungen bei der Installation und der Aktualisierung der One Identity Manager-Datenbank auf Seite 190

Einspielen eines Hotfixes in die One Identity Manager-Datenbank

WICHTIG: Bevor Sie ein Hotfixpaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung.

Hotfixpakete enthalten:

- Transportpakete, die Änderungen an der Standardkonfiguration wie beispielsweise Bildungsregeln, Skripte, Prozesse in die One Identity Manager-Datenbank enthalten

Wenn Sie mit einem Hotfixpaket ein Transportpaket erhalten, verwenden Sie das Programm Database Transporter zur Aktualisierung der One Identity Manager-Datenbank.

HINWEIS: Sollen zusätzlich zu einem Hotfixpaket weitere kundenspezifische Konfigurationsanpassungen in eine One Identity Manager-Datenbank übernommen werden, können Sie dafür mit dem Database Transporter ein kumulatives Transportpaket erstellen und dieses Transportpaket in die Zieldatenbank importieren.

- Geänderte Dateien, wie beispielsweise `*.exe`, `*.dll` oder `*.vif`

  Hotfixpakete, die geänderte Dateien enthalten, werden in der Regel als Zip-Datei bereitgestellt. Entpacken Sie die Zip-Datei und importieren Sie die geänderten Dateien mit dem Software Loader in die Datenbank. Die Dateien werden über die automatischen Softwareaktualisierung an die Arbeitsstationen und Server verteilt. Wenn Sie die automatische Softwareaktualisierung nicht einsetzen, dann aktualisieren Sie die Arbeitsstationen und Server manuell.

Detaillierte Informationen zum Thema

- Inhalt eines Transportpaketes mit dem Database Transporter anzeigen auf Seite 127
- Transportpakete mit dem Database Transporter importieren auf Seite 128
- Dateien mit dem Software Loader importieren auf Seite 130
- Transporthistorie anzeigen und One Identity Manager Version prüfen auf Seite 188
- Automatisches Aktualisieren des One Identity Manager auf Seite 101

Inhalt eines Transportpaketes mit dem Database Transporter anzeigen

Vor dem Import eines Transportpaketes mit dem Database Transporter können Sie den Inhalt der Datei anzeigen.

HINWEIS: Starten Sie den Database Transporter auf einer administrativen Arbeitsstation.

Um den Inhalt eines Transportpaketes anzuzeigen

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Änderung & Erweitern** den Eintrag **Kundenspezifische Änderungen transportieren** und klicken Sie **Starten**.

   Das Programm Database Transporter wird gestartet.
3. Auf der Startseite wählen Sie **Transportdatei anzeigen**.
4. Wählen Sie im Dateibrowser das Transportpaket und klicken Sie **Öffnen**.

5. Auf der Seite **Transportdatei auswählen** klicken Sie **Weiter**.
6. Auf der Seite **Transportdatei anzeigen** wird der Inhalt der Transportdatei angezeigt.
    - Um die Importreihenfolge der Objekte anzuzeigen
        1. Öffnen Sie über **+** einen Eintrag in der Transportdatei und wählen Sie das Kontextmenü **Sortieren nach Importreihenfolge**.
        2. Klicken Sie **OK** und erfassen Sie die Verbindungsdaten zur Datenbank. Dieser Schritt ist nur bei der ersten Ermittlung einer Reihenfolge notwendig.

           Es wird die Reihenfolge ermittelt, in der die Objekte dieses Eintrags in die Datenbank importiert werden.
        3. Wiederholen Sie Schritt a) für alle Einträge, für die Sie die Reihenfolge ermitteln möchten.
    - Um die benötigten Objekte in der Zielumgebung für einen Import anzuzeigen, wählen Sie den Eintrag für die `.xml`-Datei und wählen Sie das Kontextmenü **Abhängige Objekte anzeigen**.

      Es werden die Objekte hervorgehoben, die auf ein anderes Objekt angewiesen sind, welches nicht Teil des Transportpakets ist.
7. Um das Programm zu beenden, klicken Sie auf der letzten Seite **Fertig**.

TIPP: Sie können den Import des Transportpaketes aus dem Anzeigemodus heraus starten. Klicken Sie auf der Seite **Transportdatei anzeigen** auf den Namen des Transportpaketes und verwenden Sie das Kontextmenü **Importieren**.

Verwandte Themen

- Transportpakete mit dem Database Transporter importieren auf Seite 128

Transportpakete mit dem Database Transporter importieren

HINWEIS:

- Bevor Sie ein Transportpaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung. Verwenden Sie eine Kopie der produktiven Datenbank für die Tests.
- Um Transportpakete mit dem Database Transporter zu importieren, benötigen die Benutzer die Programmfunktion **Erlaubt den Import von Transportpaketen in die Datenbank** (`Transport_Import`).
- Starten Sie den Database Transporter auf einer administrativen Arbeitsstation.

- Für den Zeitraum des Imports wird die Datenbank in den Einzelbenutzermodus gesetzt. Beenden Sie alle bestehenden Verbindungen zur Datenbank vor dem Start des Imports.
- Beim Importieren eines Transportpaketes mit Schemaerweiterungen wird die Datenbank in den Wartungsmodus versetzt. In dieser Zeit ist die Bearbeitung von Objekten in der Datenbank nicht möglich.
- Beim Importieren eines Transportpaketes mit dem Database Transporter werden das Datum des Imports, die Beschreibung des Imports, der Versionsstand der Datenbank, der Name des Transportpaketes in der Transporthistorie der Zieldatenbank aufgezeichnet.

Um ein Transportpaket zu importieren

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Änderung & Erweitern** den Eintrag **Kundenspezifische Änderungen transportieren** und klicken Sie **Starten**.

   Das Programm Database Transporter wird gestartet.
3. Auf der Startseite wählen Sie **Transportdatei importieren**.
4. Auf der Seite **Datenbankverbindung wählen** prüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
5. Wählen Sie im Dateibrowser das Transportpaket und klicken Sie **Öffnen**.
6. Auf der Seite **Transportdatei auswählen** legen Sie Importoptionen fest.

   Tabelle 23: Importoptionen

Einstellung	Beschreibung
Protokolldatei zum Daten-import erzeugen	Um eine Protokolldatei für den Import zu erstellen, aktivieren Sie die Option. Die Protokolldatei wird im Ausgabeverzeichnis der Transportdatei abgelegt.
Objekte einzeln importieren und Fehler ignorieren	Um Objekte einzeln zu importieren, aktivieren Sie die Option. Eventuell auftretende Fehler beim Import werden ignoriert und am Ende des Importvorgangs angezeigt. Wenn Sie die Option nicht aktivieren, wird der Importvorgang bei Fehlern abgebrochen.
Standarddatendifferenzen ignorieren	Um Änderungen an Standarddaten beim Import zu ignorieren, aktivieren Sie die Option. Wenn Sie die Option nicht aktivieren, wird der Importvorgang abgebrochen, wenn Änderungen an Standarddaten enthalten sind.

7. Auf der Seite **Systemdaten importieren** werden die auszuführenden Importschritte und der Importfortschritt angezeigt. Der Importvorgang kann einige Zeit in Anspruch nehmen. Zum Abschluss werden Berechnungsaufträge für den

DBQueue Prozessor eingestellt.

HINWEIS: Stimmt beim Importieren der erwartete Wert nicht mehr mit dem aktuellen Wert in der Datenbank überein, wird der Dialog **Datenkonflikt** angezeigt. Legen Sie für jeden Konflikt fest, welcher Wert in die Datenbank übernommen werden soll.

- Wenn der Wert aus der Datenbank bestehen bleiben soll, aktivieren Sie **Aktueller Datenbankwert**.
- Wenn der Wert aus dem Transportpaket übernommen werden soll, aktivieren Sie **Transportwert**.

8. Wurden mit dem Transportpaket Änderungen an der Systemkonfiguration vorgenommen, beispielsweise Prozesse oder Skripte importiert, dann müssen Sie nach der Abarbeitung dieser Aufträge die Datenbank kompilieren. Nach dem Import wird die Kompilierung der Datenbank automatisch gestartet.
9. Um das Programm zu beenden, klicken Sie auf der letzten Seite **Fertig**.

   HINWEIS: Sind während des Importes Fehler aufgetreten, können Sie die Meldungen über die Schaltfläche speichern.

Verwandte Themen

- Inhalt eines Transportpaketes mit dem Database Transporter anzeigen auf Seite 127
- Transporthistorie anzeigen und One Identity Manager Version prüfen auf Seite 188

Dateien mit dem Software Loader importieren

WICHTIG: Bevor Sie ein Hotfixpaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung.

Um die Dateien bereitzustellen

1. Hotfixpakete, die geänderte Dateien enthalten, werden in der Regel als Zip-Datei bereitgestellt. Entpacken Sie die Zip-Datei in ein temporäres Verzeichnis auf der administrativen Arbeitsstation.
2. Kopieren Sie die Dateien in das Installationsverzeichnis der administrativen Arbeitsstation.

   Achten Sie darauf, dass die Verzeichnisstruktur erhalten bleibt. Kopieren Sie beispielsweise `*.exe`-Dateien oder `*.dll`-Dateien in das Verzeichnis `%ProgramFiles%\One Identity\One Identity Manager`. Kopieren Sie Zip-Dateien für Angular-Projekte, `Html_<MMM>.zip`, in das Verzeichnis `%ProgramFiles%\One Identity\One Identity Manager\imxweb`.
3. Starten Sie den Software Loader auf der administrativen Arbeitsstation und importieren Sie die Dateien in die One Identity Manager-Datenbank.

HINWEIS: Achten Sie im Software Loader bei der Auswahl des Basisverzeichnisses darauf, dass nicht unbeabsichtigt eine Verzeichnishierarchie erzeugt wird oder benötigte Verzeichnisse entfernt werden.

Um Dateien in eine One Identity Manager-Datenbank zu importieren

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie im Bereich **Änderung & Erweitern** den Eintrag **Dateien für Softwareaktualisierung importieren** und klicken Sie **Starten**.

   Das Programm Software Loader wird gestartet.
3. Auf der Startseite wählen Sie **In Datenbank importieren**.
4. Auf der Seite **Verbindung zur Datenbank herstellen** prüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
5. Auf der Seite **Dateien auswählen** legen Sie fest, welche Dateien importiert werden.
   a. Wählen Sie das Basisverzeichnis, in welchem sich die Dateien befinden.

      In der Dateiliste werden alle Dateien des gewählten Verzeichnisses mit ihrem Status und der Dateigröße angezeigt.

      Tabelle 24: Bedeutung der Status

Status	Bedeutung
Version unbekannt	Die Datei gehört zu den bekannten Dateien, wurde jedoch noch nicht in die Datenbank geladen. Es liegen keine Versionsinformationen in der Datenbank vor.
Datei unbekannt	Die Datei ist neu. Die Datei ist in der Liste der bekannten Dateien nicht vorhanden und wurde noch nicht in die Datenbank geladen. Es liegen keine Versionsinformationen in der Datenbank vor.
Version OK	Die Version der Datei stimmt mit der Version in der Datenbank überein.
Version geändert	Die Version der Datei hat sich gegenüber der Version in der Datenbank geändert.

   b. Markieren Sie die Dateien, die in die One Identity Manager-Datenbank zu laden sind.

      TIPP:
      - Über Mausklick auf eine Spalte im Tabellenkopf sortieren Sie die Anzeige nach der gewählten Spalte.
      - Mit **Umschalt + Auswahl** oder **Strg+ Auswahl** können Sie mehrere Dateien auswählen.

- Für eine schnelle Auswahl aller Dateien mit dem Status **Version geändert** verwenden Sie die Kontextmenüs **Alle Verzeichnisse öffnen** und **Alle geänderten Dateien öffnen**. Dateien in Unterverzeichnissen werden nur ausgewählt, wenn vorher die Verzeichnisse geöffnet wurden.

6. Auf der Seite **Änderungskennzeichen wählen** vergeben Sie ein Änderungskennzeichen, um den Austausch der Dateien zwischen verschiedenen Datenbanken, wie Testdatenbank, Entwicklungsdatenbank und produktiver Datenbank, zu erleichtern.
   a. Wählen Sie **Die Dateien sollen folgendem Änderungskennzeichen zugeordnet werden**.
   b. Wählen Sie das Änderungskennzeichen über die Schaltfläche neben der Option.
7. Die Dateien werden in die One Identity Manager-Datenbank geladen.
8. Auf der Seite **Maschinenrollen zuordnen** legen Sie weitere Einstellungen für die Dateien fest.
   a. Ordnen Sie die Dateien die Maschinenrollen zu.
   b. (Optional) Für weitere Dateieinstellungen, klicken Sie die Schaltfläche **...** neben den Dateinamen.

Tabelle 25: Weitere Dateieinstellungen

Einstellung	Beschreibung
Quellverzeichnis	Verzeichnispfad in der Installationsquelle.
Sicherungskopie erstellen	Beim der automatischen Softwareaktualisierung ist von der Datei eine Kopie anzufertigen.
Keine Aktua-lisierung	Die Datei wird durch die automatische Softwa-reaktualisierung nicht aktualisiert.

9. Um das Programm zu beenden, klicken Sie auf der letzten Seite **Ende**.

Verwandte Themen

- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- Maschinenrollen und Installationspakete auf Seite 209

Installieren zusätzlicher Module für eine bestehende One Identity Manager Installation

Um zusätzliche One Identity Manager Module zu einer bestehenden One Identity Manager Installation hinzuzufügen sind folgende Schritte erforderlich:

1. Installieren der One Identity Manager-Komponenten, die im Modul enthalten sind, auf den Arbeitsstationen und Servern.

   Aktualisieren Sie die Arbeitsstation, auf der die Schemainstallation der One Identity Manager-Datenbank gestartet wird, mit dem Installationsassistenten. Alle weiteren Arbeitstationen und Server erhalten die neuen Komponenten über die automatische Softwareaktualisierung. Für die manuelle Aktualisierung einzelner Arbeitsstationen und einzelner Server nutzen Sie den Installationsassistenten.
2. Installieren des Moduls in die One Identity Manager-Datenbank.

   WICHTIG: Hierbei handelt es sich um eine Aktualisierung der Datenbank bei der ein zusätzliches Modul gewählt wird. Bei der Nachinstallation eines Modules werden auch alle anderen Module der Datenbank verarbeitet.

   Falls Sie nachträglich Hotfixes vom Support für die Version erhalten haben, müssen Sie diese Hotfixes ebenfalls erneut installieren.

Um die Komponenten eines Moduls auf der Arbeitsstation zu installieren

1. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
2. Wechseln Sie in den Bereich **Installation**. Wählen Sie die Edition, die Sie installiert haben.
3. Klicken Sie **Installieren**.

   Der Installationsassistent wird gestartet.
4. Folgen Sie den Installationsanweisungen. Beachten Sie dabei Folgendes:
   a. Auf der Seite **Einstellungen für die Installation** erfassen Sie folgende Informationen:

- **Installationsquelle**: Wählen Sie das Verzeichnis mit den Installationsdateien.
- **Installationsverzeichnis**: Wählen Sie das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
- **Weitere Module zur gewählten Edition hinzufügen**: Aktivieren Sie die Option.

b. Auf der Seite **Modulauswahl** wählen Sie das zusätzlich zu installierende Modul.

c. Wenn Sie die Arbeitstation aktualisieren, auf der die Schemainstallation der One Identity Manager-Datenbank gestartet wird, können Sie auf der letzten Seite des Installationsassistenten, den Configuration Wizard starten.

Um die Modulerweiterungen in der One Identity Manager-Datenbank zu installieren

1. Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation.
2. Auf der Startseite des Configuration Wizard wählen Sie die Option **Datenbank aktualisieren** und klicken Sie **Weiter**.
3. Folgen Sie den Installationsanweisungen. Beachten Sie dabei Folgendes:
   a. Auf der Seite **Produktbeschreibung** werden die Konfigurationsmodule und Versionsinformationen angezeigt.
      i. Aktivieren Sie die Option **Weitere Module hinzufügen**.
      ii. Bestätigen Sie, dass von der Datenbank eine aktuelle Sicherung erstellt wurde.
      iii. Bestätigen Sie, dass die Konsistenzprüfungen der Datenbank durchgeführt wurden.
   b. Wählen Sie auf der Seite **Konfigurationsmodule auswählen** das zusätzliche Modul.

Verwandte Themen

- One Identity Manager-Komponenten mit dem Installationsassistenten aktualisieren
- Hinweise zur Aktualisierung der One Identity Manager-Datenbank auf Seite 119
- One Identity Manager-Datenbank mit dem Configuration Wizard aktualisieren

Installieren und Aktualisieren eines Anwendungsservers

Der Anwendungsserver stellt einen Verbindungspool für den Zugriff auf die Datenbank zu Verfügung. Die Clients senden ihre Anfragen an den Anwendungsserver, dieser führt die Verarbeitung der Objekte wie beispielsweise die Bildung von Werten nach definierten Bildungsregeln aus und sendet die Ergebnisse an die Clients zurück. Mit dem Speichern eines Objektes werden die Daten vom Anwendungsserver an die Datenbank übergeben.

Stellen Sie vor der Installation sicher, dass die minimalen Hardware- und Softwarevoraussetzungen auf dem Server erfüllt sind.

HINWEIS: Auf Linux Betriebssystemen wird die Verwendung des Docker-Images oneidentity/oneim-appserver empfohlen.

Detaillierte Informationen zum Thema

- Minimale Systemanforderungen für den Anwendungsserver auf Seite 44
- Hinweise zum Installieren eines Anwendungsservers auf Seite 135
- Anwendungsserver installieren auf Seite 136
- Status eines Anwendungsservers anzeigen auf Seite 141
- Suchindex auf Anwendungsservern aktualisieren auf Seite 143
- Anwendungsserver aktualisieren auf Seite 141
- Anwendungsserver deinstallieren auf Seite 144

Hinweise zum Installieren eines Anwendungsservers

- Wenn Sie den One Identity Manager Service oder den Designer über einen Anwendungsserver betreiben wollen, dann benötigt der Anwendungsserver mindestens die Berechtigungen eines Konfigurationsbenutzers. Verwenden Sie bei

der Installation des Anwendungsservers für die Verbindung zur One Identity Manager-Datenbank und zur Authentifizierung gegen die One Identity Manager-Datenbank die SQL Server Anmeldung für den Konfigurationsbenutzer.

- Um die Berechtigungen für Endbenutzer einzuschränken, können Sie einen weiteren Anwendungsserver bereitstellen, der die SQL Server Anmeldung für Endbenutzer verwendet.
- Um ein Web Portal zu betreiben oder die Volltextsuche im Manager zu nutzen, benötigen Sie einen Anwendungsserver mit installiertem Suchdienst.
- Starten Sie die Installation des Anwendungsservers lokal auf dem Server.
- 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.

Anwendungsserver installieren

WICHTIG: Starten Sie die Installation des Anwendungsservers lokal auf dem Server.

HINWEIS: Auf Linux Betriebssystemen wird die Verwendung des Docker-Images oneidentity/oneim-appserver empfohlen.

Um einen Anwendungsserver zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:
   a. Wechseln Sie zum Tabreiter **Installation**.
   b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

   Der Web Installer wird gestartet.
3. Auf der Startseite des Web Installer wählen Sie **Anwendungsserver installieren** und klicken Sie **Weiter**.
4. Auf der Seite **Datenbankverbindung** nehmen Sie eine der folgenden Aktionen vor:
   - Um eine bestehende Verbindung zur One Identity Manager-Datenbank zu verwenden, wählen Sie in der Auswahlliste **Datenbankverbindung auswählen** die entsprechende Verbindung aus.

     - ODER -
   - Um eine neue Verbindung zur One Identity Manager-Datenbank zu verwenden, klicken Sie **Neue Verbindung erstellen** und geben Sie eine neue Verbindung an.
5. Unter **Authentifizierungsverfahren** geben Sie das Verfahren und die Anmeldedaten an, mit denen Sie sich an der Datenbank anmelden möchten.

6. Auf der Seite **Installationsziel wählen** nehmen Sie die folgenden Einstellungen vor.

Tabelle 26: Einstellungen für das Installationsziel

Einstellung	Beschreibung
Anwendungsname	Name, der als Anwendungsname zum Beispiel in der Titelzeile des Browsers verwendet werden soll.
Zielpfad im IIS	Webseite auf dem Internet Information Services, auf dem die Anwendung installiert wird.
SSL erzwingen	Gibt an, ob sichere oder unsichere Webseiten zur Installation angeboten werden. Ist die Option aktiviert, können nur Seiten, die per SSL gesichert sind, zur Installation verwendet werden. Diese Einstellung ist der Standardwert. Ist die Option nicht aktiviert, können unsichere Webseiten zur Installation verwendet werden.
URL	Uniform Resource Locator (URL) der Anwendung.
Dedizierten Anwendungspool einrichten	Gibt an, ob für jede Anwendung ein eigener Anwendungspool installiert werden soll. Diese Option ermöglicht es, Anwendungen unabhängig voneinander einzustellen. Ist die Option aktiviert, wird jede Anwendung in ihren eigenen Anwendungspool installiert.
Anwendungspool	Anwendungspool, der verwendet werden soll. Die Angabe ist nur möglich, wenn die Option **Dedizierter Anwendungspool einrichten** deaktiviert ist. Wenn Sie den Standardwert **DefaultAppPool** verwenden, wird der Anwendungspool nach folgender Syntax gebildet: `<Anwendungsname>_POOL`
Identität	Berechtigung für die Ausführung des Anwendungspool. Sie können eine Standard-Identität oder ein benutzerdefiniertes Benutzerkonto verwenden. Wenn Sie den Standardwert **ApplicationPoolIdentity** verwenden, wird das Benutzerkonto nach folgender Syntax gebildet: `IIS APPPOOL\<Anwendungsname>_POOL` Wenn Sie einen anderen Benutzer berechtigen möchten, klicken Sie **...** neben dem Eingabefeld, aktivieren Sie die Option **Benutzerdefiniertes Konto** und erfassen Sie den Benutzer und sein Kennwort.
Web-Authen-	Authentifizierungsart gegenüber der Webanwendung. Zur

Einstellung	Beschreibung
tifizierung	Auswahl stehen: • **Windows Authentifizierung (Single Sign-On)** Der Benutzer wird gegenüber dem Internet Information Services mithilfe seines Windows-Benutzerkontos authentifiziert und die Webanwendung meldet die diesem Benutzerkonto zugeordnete Person rollenbasiert an. Sollte dieses Single Sign-on nicht möglich sein, wird der Benutzer auf eine Anmeldeseite umgeleitet. Diese Authentifizierung ist nur wählbar, wenn die Windows-Authentifizierung installiert ist. • **Anonym** Eine Anmeldung ohne Windows-Authentifizierung ist möglich. Der Benutzer wird gegenüber dem Internet Information Services und der Webanwendung anonym authentifiziert und die Webanmeldung leitet auf eine Anmeldeseite um.
Datenbank-Authen-tifizierung	HINWEIS: Dieser Bereich wird Ihnen nur angezeigt, wenn Sie auf der Seite **Datenbankverbindung** eine SQL-Datenbankverbindung ausgewählt haben. Authentifizierungsart gegenüber der One Identity Manager-Datenbank. Zur Auswahl stehen: • **Windows Authentifizierung** Die Webanwendung authentifiziert sich gegenüber der One Identity Manager-Datenbank mit dem Windows-Benutzerkonto, unter dem ihr Anwendungspool läuft. Eine Anmeldung ist über ein benutzerdefiniertes Benutzerkonto oder einer Standard-Identität für den Anwendungspool möglich. • **SQL-Authentifizierung** Die Authentifizierung erfolgt mittels SQL Server-Anmeldung und Kennwort. Es wird die SQL Server-Anmeldung aus der Verbindung zur Datenbank verwendet. Über die Schaltfläche [**...**] können Sie eine abweichende SQL-Anmeldung angeben, beispielsweise wenn die Anwendung mit einer Berechtigungsebene für Endbenutzer ausgeführt werden soll. Diese Zugangsdaten werden maschinenspezifisch verschlüsselt in der Konfiguration der Webanwendung gespeichert.

7. Auf der Seite **Maschinenrollen zuordnen** legen Sie die Maschinenrollen fest.

Die Maschinenrollen für den Anwendungsserver sind aktiviert. Die Maschinenrollen **Search Service** und **Search Indexing Service** werden für die Suchindizierung für die Volltextsuche benötigt. Diese Maschinenrollen sind immer gemeinsam zu verwenden.

HINWEIS: Wenn Sie ein Web Portal nutzen möchten, wird ein Anwendungsserver benötigt, auf dem der Suchdienst installiert ist.

8. Auf der Seite **Setze das Session-Token-Zertifikat** wählen Sie das Zertifikat, das für die Erstellung und Prüfung von Sitzungstoken verwendet wird.

   HINWEIS: Das Zertifikat muss mindestens eine Schlüssellänge von 1024 Bit haben.

   - Um ein bestehendes Zertifikat zu verwenden, nehmen Sie die folgenden Einstellungen vor.
     1. **Zertifikat für das Session-Token**: Wählen Sie den Eintrag **Nutze bestehendes Zertifikat**.
     2. **Zertifikat auswählen**: Wählen Sie das Zertifikat.

        HINWEIS: Es wird dringend empfohlen, das bereits in anderen Anwendungsservern und API Servern zum Einsatz kommende Zertifikat hier ebenfalls zu nutzen.
   - Um ein neues Zertifikat zu erzeugen, nehmen Sie die folgenden Einstellungen vor.
     1. **Zertifikat für das Session-Token**: Wählen Sie den Eintrag **Erzeuge neues Zertifikat**.
     2. **Zertifikatsherausgeber**: Erfassen Sie den Aussteller des Zertifikats.
     3. **Schlüssellänge**: Legen Sie die Schlüssellänge für das Zertifikat fest.

     Das Zertifikat wird in die Zertifikatsverwaltung des Anwendungsservers eingetragen.

     HINWEIS: Es wird dringend empfohlen, dieses neu erstellte Zertifikat zu exportieren und in anderen Anwendungsservern und API Servern ebenfalls einzusetzen, sodass alle diese Server-Komponenten über das identische Session-Zertifikat verfügen und dieses nutzen.
   - Um eine neue Zertifikatsdatei zu erzeugen, nehmen Sie die folgenden Einstellungen vor.
     1. **Zertifikat für das Session-Token**: Wählen Sie den Eintrag **Erzeuge neue Zertifikatsdatei**.
     2. **Zertifikatsherausgeber**: Erfassen Sie unter den Aussteller des Zertifikats.
     3. **Schlüssellänge**: Legen Sie die Schlüssellänge für das Zertifikat fest.
     4. **Zertifikatsdatei**: Tragen Sie den Ablagepfad und Namen der Zertifikatsdatei ein.

     Die Zertifikatsdatei wird im angegebenen Verzeichnis der Webanwendung abgelegt.

HINWEIS: Es wird dringend empfohlen, dieses neu erstellte Zertifikat in anderen Anwendungsservern und API Servern ebenfalls einzusetzen, sodass alle diese Server-Komponenten über das identische Session-Zertifikat verfügen und dieses nutzen.

9. Auf der Seite **Setze das Konto für Aktualisierung** legen Sie das Benutzerkonto für die automatische Aktualisierung fest. Das Benutzerkonto wird verwendet, um die Dateien im Anwendungsverzeichnis anzulegen oder auszutauschen.
   - **Nutze die IIS-Berechtigungen für Aktualisierungen**: Um das Benutzerkonto, unter welchem der Anwendungspool ausgeführt wird, für die Aktualisierungen zu nutzen, aktivieren Sie die Option.
   - **Nutze ein spezielles Konto für die Aktualisierungen**: Um ein anderes Benutzerkonto zu verwenden, aktivieren Sie die Option. Geben Sie die Domäne, den Benutzernamen und das Kennwort des Benutzers an.
10. (Optional) Für die Auswertung von archivierten Daten in Berichten und im TimeTrace wird auf eine One Identity Manager History Database zugegriffen. Wenn der Zugriff auf die One Identity Manager History Database über einen Anwendungsserver erfolgen soll, erfassen Sie auf der Seite **History Database-Verbindungen bearbeiten** die Kennung und die Verbindungsparameter zur One Identity Manager History Database.

    HINWEIS: Sie können die Verbindungsinformationen zu einer One Identity Manager History Database auch zu einem späteren Zeitpunkt hinzufügen. Dazu passen Sie die Konfigurationsdatei (`web.config`) an.

    Ausführliche Informationen zur Verbindung zur One Identity Manager History Database über Anwendungsserver und die erforderliche Konfiguration finden Sie im *One Identity Manager Administrationshandbuch für die Datenarchivierung*.
11. Auf der Seite **Installation läuft** werden die einzelnen Installationsschritte angezeigt. Nachdem der Vorgang abgeschlossen wurde, klicken Sie **Weiter**.
12. Auf der letzten Seite klicken Sie **Fertig**, um das Programm zu beenden.
13. Schließen Sie das Autorun-Programm.

HINWEIS: Der Web Installer generiert die Webanwendung und die Konfigurationsdatei (`web.config`). Der Web Installer verwendet Standardwerte für die Konfigurationseinstellungen. Sie können diese Werte beibehalten. Es wird empfohlen, dass Sie die Einstellungen überprüfen. Die Konfigurationsdatei (`web.config`) finden Sie im Verzeichnis der Webanwendung im Internet Information Services.

Verwandte Themen

- Minimale Systemanforderungen für den Anwendungsserver auf Seite 44
- Hinweise zum Installieren eines Anwendungsservers auf Seite 135
- Status eines Anwendungsservers anzeigen auf Seite 141
- Anwendungsserver aktualisieren auf Seite 141
- Benutzer mit abgestuften Berechtigungen für die One Identity Manager-Datenbank

auf einem SQL Server auf Seite 29
- Maschinenrollen und Installationspakete auf Seite 209

Status eines Anwendungsservers anzeigen

Der Anwendungsserver ist über ein Browserfrontend erreichbar.

Der Aufruf erfolgt mit der entsprechenden URL:

http://<Servername>/<Anwendungsname>

https://<Servername>/<Anwendungsname>

TIPP: Sie können die Statusanzeige des Webservers im Job Queue Info öffnen. Wählen Sie dazu im Job Queue Info das Menü **Ansicht > Serverstatus** und öffnen Sie auf dem Tabreiter **Webserver** die Statusanzeige des Webservers über das Kontextmenü **Im Browser öffnen**.

Für den Anwendungsserver werden verschiedene Statusinformationen angezeigt. Die Statusinformationen des Anwendungsservers stehen auch als Leistungsindikatoren zur Verfügung. Benutzer mit der Programmfunktion **Aktiviert die Protokollanzeige im Anwendungsserver** (`AppServer_Logs`) sehen das Protokoll.

Zusätzlich ist hier eine API Dokumentation verfügbar. Um auf die REST API im Anwendungsserver zuzugreifen, benötigen die Benutzer die Programmfunktion **Erlaubt den Zugriff auf die REST API des Anwendungsservers** (`AppServer_API`). Ausführliche Informationen zur REST API finden Sie im *One Identity Manager REST API Reference Guide*.

Anwendungsserver aktualisieren

HINWEIS:

- Es wird empfohlen die automatische Aktualisierung nur in speziellen Wartungsfenstern durchzuführen, in denen die Anwendung von den Benutzern nicht erreichbar ist und der Neustart der Anwendung gefahrlos manuell durchgeführt werden kann.
- Für die automatische Aktualisierung sind folgende Berechtigungen erforderlich:
  - Das Benutzerkonto für die Aktualisierung benötigt die Berechtigung zum Schreiben auf das Anwendungsverzeichnis.
  - Das Benutzerkonto für die Aktualisierung benötigt die lokale Sicherheitsrichtlinie **Anmelden als Stapelverarbeitungsauftrag**.

- Das Benutzerkonto, unter dem der Anwendungspool läuft, benötigt die lokalen Sicherheitsrichtlinien **Ersetzen eines Tokens auf Prozessebene** und **Anpassen von Speicherkontingenten für einen Prozess**.

Um eine Aktualisierung durchzuführen, sind zunächst die zu aktualisierenden Dateien in die One Identity Manager-Datenbank einzuspielen. Die benötigten Dateien werden beim Einspielen eines Hotfixes, eines Service Packs oder einer Versionsänderung in die One Identity Manager-Datenbank eingefügt und aktualisiert.

Die Prüfung erfolgt abhängig vom gewählten Modus für die automatische Aktualisierung. Werden neue Dateien erkannt, so werden diese aus der Datenbank geladen. Die Dateien können nicht aktualisiert werden, solange die Anwendung läuft. Die Aktualisierung wartet bis die Anwendung neu gestartet wird.

Der Neustart der Anwendung erfolgt durch den Webserver automatisch, wenn die Anwendung eine definierte Zeitspanne keine Benutzeraktivität aufweist. Dies kann aber einige Zeit dauern oder durch ununterbrochene Benutzeranfragen verhindert werden.

Die automatische Aktualisierung konfigurieren Sie in der Datei `web.config` des Anwendungsservers. In der Sektion`<autoupdate>` können Sie das Verhalten für die Aktualisierung beeinflussen.

Tabelle 27: Attribute für die Konfiguration der automatischen Aktualisierung

Attibut	Beschreibung
off	Gibt an, ob die automatische Aktualisierung deaktiviert ist (**True**) oder aktiviert ist (**False**).
mode	Modus für die automatische Aktualisierung. Zulässige Werte sind: • **timer**: Zeitgesteuerte Prüfung (Standard). Die Prüfung auf aktualisierte Dateien in der Datenbank erfolgt bei Start der Anwendung und wird danach im definierten Prüfintervall (Attribut `checkinterval`) durchgeführt. • **manual**: Manuell Prüfung. Die Prüfung wird über die Statusseite des Anwendungsservers gestartet. Eine regelmäßige Prüfung auf aktualisierte Dateien in der Datenbank findet nicht statt.
checkinterval	Zeitspanne, nach der im Modus **timer** nach Aktualisierungen gesucht wird. Standard: **5** Minuten
inactivitytime	Zeitspanne, in der keine Benutzeraktivität erfolgen darf, damit die Aktualisierung gestartet werden kann. Standard: **10** Sekunden.

Beispiel:

```
<autoupdate>
     <!-- <add key="off" value="true" /> -->
```

```
      <add key="mode" value="timer" /> <!-- Valid options: timer, manual -->
      <add key="checkinterval" value="00:05:00"/>
      <add key="inactivitytime" value="00:00:10"/>
</autoupdate>
```

Um die Aktualisierung manuell zu starten

1. Öffnen Sie die Statusseite des Anwendungsservers im Browser.
2. Klicken Sie im Menü des angemeldeten Benutzers **Update immediately**.

Verwandte Themen

- Status eines Anwendungsservers anzeigen auf Seite 141
- Automatisches Aktualisieren des One Identity Manager auf Seite 101

Suchindex auf Anwendungsservern aktualisieren

Bei Änderungen an einer Tabelle mit indizierten Spalten, den referenzierten Tabellen oder den Übersetzungen wird der Suchindex aktualisiert.

Über den Konfigurationsparameter **Common | Indexing | BatchSize** legen Sie fest, wie viele Objekte in einem Indizierungslauf maximal indiziert werden. Der Standardwert ist **50000**.

Der Konfigurationsparameter **Common | Indexing | Interval** enthält das Intervall zwischen zwei Indizierungsläufen. Standardwert sind **120** Sekunden. Nach Ablauf dieses Intervalls wird ein neuer Indizierungslauf gestartet.

Sie können den Suchindex manuell aktualisieren.

Um den Suchindex auf dem Anwendungsserver manuell zu aktualisieren

1. Öffnen Sie die Statusseite des Anwendungsservers im Browser.
2. Klicken Sie im Menü des angemeldeten Benutzers **Update Index**.
3. Wählen Sie, ob alle Indexe oder nur geänderte Indexe aktualisiert werden sollen.

Verwandte Themen

- Status eines Anwendungsservers anzeigen auf Seite 141
- Meldungen zur Indizierung des Suchindex auf Seite 197

Anwendungsserver deinstallieren

Um eine Webanwendung zu deinstallieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:
   a. Wechseln Sie zum Tabreiter **Installation**.
   b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

   Der Web Installer wird gestartet.
3. Auf der Startseite des Web Installer klicken Sie **Deinstallieren einer Webanwendung** und klicken Sie **Weiter**.
4. Auf der Seite **Deinstallieren einer Webanwendung** doppelklicken Sie die Webanwendung, die Sie entfernen möchten.

   Vor der Anwendung wird das Symbol angezeigt.
5. Klicken Sie **Weiter**.
6. Auf der Seite **Datenbankverbindung** wählen Sie die Datenbankverbindung und das Authentifizierungsverfahren und geben Sie die entsprechenden Anmeldedaten ein.
7. Klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installation läuft** werden die einzelnen Schritte zur Deinstallation angezeigt.
10. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
11. Auf der Seite **Beenden des Assistenten** klicken Sie **Fertig**.
12. Schließen Sie das Autorun-Programm.

Installieren des API Servers

Der API Server hostet die API, die Sie definiert haben. Über den API Server werden zudem Angular-Web-Apps ausgeliefert.

Sie können den API Server mithilfe des Web Installers oder des ImxClient-Kommandozeilenprogramms installieren (Kommando **install-apiserver**). Lesen Sie in den nachfolgenden Abschnitten, wie Sie den API Server mithilfe des Web Installers auf einem Windows Server installieren und in der Standardkonfiguration in Betrieb nehmen. Weitere Informationen über die Installation mithilfe des ImxClient-Kommandozeilenprogramms finden Sie im *One Identity Manager API-Entwicklungshandbuch*.

Detaillierte Informationen zum Thema

- Minimale Systemanforderungen für den Webserver auf Seite 42
- API Server installieren auf Seite 145
- API Server deinstallieren auf Seite 150

API Server installieren

WICHTIG: Starten Sie die Installation des API Servers lokal auf dem Server.

HINWEIS: Stellen Sie vor der Installation sicher, dass die minimalen Hardware- und Software-Voraussetzungen auf dem Server gewährleistet sind.

HINWEIS: Auf Linux Betriebssystemen wird die Verwendung des Docker-Images oneidentity/oneim-api empfohlen.

TIPP: Sie können den API Server auch mithilfe des ImxClient-Kommandozeilenprogramms (Kommando **install-apiserver**) installieren. Weitere Informationen finden Sie im *One Identity Manager API-Entwicklungshandbuch*.

Um den API Server zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten nehmen Sie folgende Aktionen vor:

a. Klicken Sie **Installation**.

b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

Der Web Installer wird gestartet.

3. Auf der Startseite des Web Installers klicken Sie **API Server installieren**.
4. Klicken Sie **Weiter**.
5. Auf der Seite **Datenbankverbindung** nehmen Sie eine der folgenden Aktionen vor:

   TIPP: One Identityempfiehlt die Verwendung einer Verbindung über einen Anwendungsserver.

   - Um eine bestehende Verbindung zur One Identity Manager-Datenbank zu verwenden, wählen Sie in der Auswahlliste **Datenbankverbindung auswählen** die entsprechende Verbindung aus.
   - Um eine neue Verbindung zur One Identity Manager-Datenbank zu verwenden, klicken Sie **Neue Verbindung erstellen** und geben Sie eine neue Verbindung an.
6. Unter **Authentifizierungsverfahren** geben Sie das Verfahren und die Anmeldedaten an, mit denen Sie sich an der Datenbank anmelden möchten.
7. Klicken Sie **Weiter**.
8. Auf der Seite **Installationsquelle** nehmen Sie eine der folgenden Aktionen vor:
   - Um die Installationsdaten aus der Datenbank zu beziehen, aktivieren Sie die Option **Datenbank**.
   - Um die Installationsdaten aus dem Installationsmedium (beispielsweise von der Festplatte) zu beziehen, aktivieren Sie die Option **Dateisystem** und geben Sie einen Pfad an.
9. Klicken Sie **Weiter**.
10. Auf der Seite **Installationsziel wählen** nehmen Sie die folgenden Einstellungen vor:

Tabelle 28: Einstellungen für das Installationsziel

Einstellung	Beschreibung
Anwendungsname	Geben Sie den Namen ein, der als Anwendungsname im Browser verwendet werden soll.
Zielpfad im IIS	Wählen Sie die Webseite auf dem Internet Information Services, auf dem die Anwendung installiert wird.
SSL erzwingen	Aktivieren Sie das Kontrollkästchen, falls die API Server-Webseite nur über eine verschlüsselte Verbindung aufgerufen werden darf.
URL	Geben Sie die URL der Anwendung ein.
Dedizierten Anwen-	Aktivieren Sie das Kontrollkästchen, falls für jede

Einstellung	Beschreibung
dungspool einrichten	Anwendung ein eigener Anwendungspool installiert werden soll. Diese Option ermöglicht es, Anwendungen unabhängig voneinander einzustellen. Ist die Option aktiviert, wird jede Anwendung in ihren eigenen Anwendungspool installiert.
Anwendungspool	Wählen Sie den Anwendungspool aus, der verwendet werden soll. Die Angabe ist nur möglich, wenn das Kontrollkästchen **Dedizierter Anwendungspool einrichten** deaktiviert ist. Wenn Sie den Standardwert **DefaultAppPool** verwenden, wird der Anwendungspool nach folgender Syntax gebildet: `<Anwendungsname>_POOL`
Identität	Legen Sie die Berechtigung für die Ausführung des Anwendungspools fest. Sie können eine Standard-Identität oder ein benutzerdefiniertes Benutzerkonto verwenden. Wenn Sie den Standardwert **ApplicationPoolIdentity** verwenden, wird das Benutzerkonto nach folgender Syntax gebildet: `IIS APPPOOL\<Anwendungsname>_POOL` Wenn Sie einen anderen Benutzer berechtigen möchten, klicken Sie neben dem Eingabefeld auf **...**, aktivieren Sie die Option **Benutzerdefiniertes Konto** und geben Sie den Benutzer und sein Kennwort ein.
Web-Authentifizierung	Legen Sie fest, welche Authentifizierungsart gegenüber der Webanwendung verwendet werden soll. Zur Auswahl stehen: • **Windows Authentifizierung (Single Sign-On)** Der Benutzer wird gegenüber dem Internet Information Services mithilfe seines Windows-Benutzerkontos authentifiziert und die Webanwendung meldet die diesem Benutzerkonto zugeordnete Person rollenbasiert an. Sollte dieses Single Sign-on nicht möglich sein, wird der Benutzer auf eine Anmeldeseite umgeleitet. Diese Authentifizierung ist nur wählbar, wenn die Windows-Authentifizierung installiert ist. • **Anonym** Eine Anmeldung ohne Windows-Authentifizierung ist möglich. Der Benutzer wird gegenüber dem Internet Information Services und der Webanwendung anonym authentifiziert und die Webanmeldung leitet auf eine Anmeldeseite um.

Einstellung	Beschreibung
Datenbank-Authentifizierung	HINWEIS: Dieser Bereich wird Ihnen nur angezeigt, wenn Sie auf der Seite **Datenbankverbindung** eine SQL-Datenbankverbindung ausgewählt haben. Legen Sie fest, welche Authentifizierungsart gegenüber der One Identity Manager-Datenbank verwendet werden soll. Zur Auswahl stehen: • **Windows Authentifizierung** Die Webanwendung authentifiziert sich gegenüber der One Identity Manager-Datenbank mit dem Windows-Benutzerkonto, unter dem ihr Anwendungspool läuft. Eine Anmeldung ist über ein benutzerdefiniertes Benutzerkonto oder einer Standard-Identität für den Anwendungspool möglich. • **SQL-Authentifizierung** Eine Anmeldung ist nur über ein benutzerdefiniertes Benutzerkonto möglich. Die Authentifizierung erfolgt mittels Benutzername und Kennwort. Diese Zugangsdaten werden maschinenspezifisch verschlüsselt in der Konfiguration der Webanwendung gespeichert.

11. Klicken Sie **Weiter**.

    Wenn Sie zuvor eine direkte Datenbankverbindung ausgewählt haben, wird Ihnen die Seite **Anwendungsserver wählen** angezeigt.

12. (Optional) Auf der Seite **Anwendungsserver wählen** nehmen Sie die folgenden Aktionen vor:

    HINWEIS: Wenn Sie die Volltextsuche verwenden möchten, müssen Sie einen Anwendungsserver angeben. Sie können den Anwendungsserver auch zu einem späteren Zeitpunkt in die Konfigurationsdatei eintragen.

    a. Klicken Sie **Anwendungsserver eintragen**.

    b. Im Dialogfenster im Feld **URL** geben Sie die Webadresse des Anwendungsservers ein.

    c. Klicken Sie **OK**.

13. Klicken Sie **Weiter**.

14. Auf der Seite **Setze das Session-Token-Zertifikat** wählen Sie das Zertifikat, das für die Erstellung und Prüfung von Sitzungstoken verwendet wird.

    HINWEIS: Das Zertifikat muss mindestens eine Schlüssellänge von 1024 Bit haben.

    • Um ein bestehendes Zertifikat zu verwenden, nehmen Sie die folgenden Einstellungen vor.

1. **Zertifikat für das Session-Token**: Wählen Sie den Eintrag **Nutze bestehendes Zertifikat**.
2. **Zertifikat auswählen**: Wählen Sie das Zertifikat.

   HINWEIS: Es wird dringend empfohlen, das bereits in anderen Anwendungsservern und API Servern zum Einsatz kommende Zertifikat hier ebenfalls zu nutzen.

- Um ein neues Zertifikat zu erzeugen, nehmen Sie die folgenden Einstellungen vor.
  1. **Zertifikat für das Session-Token**: Wählen Sie den Eintrag **Erzeuge neues Zertifikat**.
  2. **Zertifikatsherausgeber**: Erfassen Sie den Aussteller des Zertifikats.
  3. **Schlüssellänge**: Legen Sie die Schlüssellänge für das Zertifikat fest.

  Das Zertifikat wird in die Zertifikatsverwaltung des Anwendungsservers eingetragen.

  HINWEIS: Es wird dringend empfohlen, dieses neu erstellte Zertifikat zu exportieren und in anderen Anwendungsservern und API Servern ebenfalls einzusetzen, sodass alle diese Server-Komponenten über das identische Session-Zertifikat verfügen und dieses nutzen.
- Um eine neue Zertifikatsdatei zu erzeugen, nehmen Sie die folgenden Einstellungen vor.
  1. **Zertifikat für das Session-Token**: Wählen Sie den Eintrag **Erzeuge neue Zertifikatsdatei**.
  2. **Zertifikatsherausgeber**: Erfassen Sie unter den Aussteller des Zertifikats.
  3. **Schlüssellänge**: Legen Sie die Schlüssellänge für das Zertifikat fest.
  4. **Zertifikatsdatei**: Tragen Sie den Ablagepfad und Namen der Zertifikatsdatei ein.

  Die Zertifikatsdatei wird im angegebenen Verzeichnis der Webanwendung abgelegt.

  HINWEIS: Es wird dringend empfohlen, dieses neu erstellte Zertifikat in anderen Anwendungsservern und API Servern ebenfalls einzusetzen, sodass alle diese Server-Komponenten über das identische Session-Zertifikat verfügen und dieses nutzen.

15. Klicken Sie **Weiter**.
16. Auf der Seite **Maschinenrollen zuordnen** legen Sie die Maschinenrollen fest.

    Die Maschinenrolle **SCIM Provider** wird für das SCIM Plugin im API Server benötigt. Ausführliche Informationen zum SCIM Plugin finden Sie im *One Identity Manager Konfigurationshandbuch*.
17. Klicken Sie **Weiter**.

18. Auf der Seite **Setze das Konto für Aktualisierung** legen Sie das Benutzerkonto für die automatische Aktualisierung fest, indem Sie eine der folgenden Optionen aktivieren:

    HINWEIS: Das Benutzerkonto wird verwendet, um die Dateien im Anwendungsverzeichnis anzulegen oder auszutauschen.

    - **Nutze die IIS-Berechtigungen für Aktualisierungen**: Um das Benutzerkonto, unter dem der Anwendungspool ausgeführt wird, für die Aktualisierungen zu nutzen, aktivieren Sie diese Option.
    - **Nutze ein spezielles Konto für die Aktualisierungen**: Um ein anderes Benutzerkonto zu verwenden, aktivieren Sie diese Option. Geben Sie die Domäne, den Benutzernamen und das Kennwort des Benutzers an.

19. Klicken Sie **Weiter**.
20. Auf der Seite **Anwendungstoken** geben Sie im Eingabefeld das Anwendungstoken für den API Server ein.

    TIPP: Um ein neues Token zu verwenden und das bestehende Token in der Datenbank zu ersetzen, aktivieren Sie die Option **Ersetze das Anwendungstoken in der Datenbank**. Beachten Sie dabei, dass das bisherig verwendete Token an allen bereits verwendeten Stellen ungültig wird und Sie diese Stellen gegebenenfalls mit dem neuen Token aktualisieren müssen.

    HINWEIS: Behandeln Sie das Anwendungstoken wie ein Kennwort. Sobald das Anwendungstoken in der Datenbank gespeichert wird, kann es nicht mehr im Klartext angezeigt werden. Notieren Sie sich das Anwendungstoken gegebenenfalls.

21. Klicken Sie **Weiter**.

    Die Seite **Installation läuft** öffnet sich und zeigt die einzelnen Installationsschritte.
22. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
23. Auf der Seite **Beenden des Assistenten** klicken Sie **Fertig**.
24. Schließen Sie das Autorun-Programm.

Verwandte Themen

- API Server deinstallieren auf Seite 150

API Server deinstallieren

Um eine Webanwendung zu deinstallieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:

a. Wechseln Sie zum Tabreiter **Installation**.

b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

Der Web Installer wird gestartet.

3. Auf der Startseite des Web Installer klicken Sie **Deinstallieren einer Webanwendung** und klicken Sie **Weiter**.
4. Auf der Seite **Deinstallieren einer Webanwendung** doppelklicken Sie die Webanwendung, die Sie entfernen möchten.

   Vor der Anwendung wird das Symbol angezeigt.
5. Klicken Sie **Weiter**.
6. Auf der Seite **Datenbankverbindung** wählen Sie die Datenbankverbindung und das Authentifizierungsverfahren und geben Sie die entsprechenden Anmeldedaten ein.
7. Klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installation läuft** werden die einzelnen Schritte zur Deinstallation angezeigt.
10. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
11. Auf der Seite **Beenden des Assistenten** klicken Sie **Fertig**.
12. Schließen Sie das Autorun-Programm.

Verwandte Themen

- API Server installieren auf Seite 145

11

Installieren, Konfigurieren und Warten des Web Designer Web Portals

Mit Hilfe des Web Installers können Sie das Web Designer Web Portal installieren, konfigurieren und aktualisieren. Nachfolgend wird auf die Schritte eingegangen, die nötig sind, um das Web Designer Web Portal auf einem Windows Server zu installieren und in der Standardkonfiguration in Betrieb zu nehmen. Die Konfigurationseinstellungen werden mit ihren entsprechend möglichen Werten erläutert.

Detaillierte Informationen zum Thema

Web Designer Web Portal installieren

Lesen Sie nachfolgend, wie Sie das Web Designer Web Portal installieren. Beachten Sie zudem folgende Hinweise:

HINWEIS:

- Stellen Sie vor der Installation sicher, dass die minimalen Hardware- und Software-Voraussetzungen auf dem Server gewährleistet sind.
- Stellen Sie einen Anwendungsserver bereit, auf dem der Suchdienst für das Web Designer Web Portalinstalliert ist.
- Starten Sie die Installation des Web Designer Web Portal lokal auf dem Server.

- Wenn Sie das Web Designer Web Portal mit HTTPS installieren, wird die Übertragungsart der Cookies in HTTPS im Web Installer eingerichtet.
- Wenn Sie Änderungen der SSL-Einstellungen am Web Designer Web Portal zu einem späteren Zeitpunkt vornehmen, müssen Sie den Wert manuell in der Konfigurationsdatei `web.config` des Web Portals anpassen.
- Bei der Installation werden Standardwerte für die Konfigurationseinstellungen verwendet. Sie können diese Werte beibehalten. Überprüfen Sie die Einstellungen mithilfe des Web Designer Configuration Editors.

  Um eine Änderung vorzunehmen

  - Schreiben Sie zum Beispiel den Wert `<httpCookies requireSSL="true">` in die `web.config` unter dem Element `<system.web>`.

HINWEIS: Auf Linux Betriebssystemen wird die Verwendung des Docker-Images oneidentity/oneim-web empfohlen.

Um das Web Designer Web Portal zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:
   a. Wechseln Sie zum Tabreiter **Installation**.
   b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

   Der Web Installer wird gestartet.
3. Auf der Startseite des Web Installers klicken Sie **Web Portal installieren** und klicken Sie **Weiter**.
4. Auf der Seite **Datenbankverbindung** nehmen Sie eine der folgenden Aktionen vor:
   - Um eine bestehende Verbindung zur One Identity Manager-Datenbank zu verwenden, wählen Sie aus der Auswahlliste **Datenbankverbindung auswählen** die entsprechende Verbindung.

     - ODER -
   - Um eine neue Verbindung zur One Identity Manager-Datenbank zu verwenden, klicken Sie **Neue Verbindung erstellen** und geben Sie eine neue Verbindung an (siehe Datenbankverbindung konfigurieren auf Seite 160).
5. Unter **Authentifizierungsverfahren** geben Sie das Verfahren und die Anmeldedaten an, mit denen Sie sich an der Datenbank anmelden möchten.
6. Klicken Sie **Weiter**.
7. Auf der Seite **Installationsziel wählen** nehmen Sie die folgenden Einstellungen vor:

Tabelle 29: Einstellungen für das Installationsziel

Einstellung	Beschreibung
Anwendungsname	Name, der als Anwendungsname zum Beispiel in der Titelzeile des Browsers verwendet werden soll.
Zielpfad im IIS	Webseite auf dem Internet Information Services, auf dem die Anwendung installiert wird.
SSL erzwingen	Gibt an, ob sichere oder unsichere Webseiten zur Installation angeboten werden. Ist die Option aktiviert, können nur Seiten, die per SSL gesichert sind, zur Installation verwendet werden. Diese Einstellung ist der Standardwert. Ist die Option nicht aktiviert, können unsichere Webseiten zur Installation verwendet werden.
URL	Uniform Resource Locator (URL) der Anwendung.
Dedizierten Anwendungspool einrichten	Gibt an, ob für jede Anwendung ein eigener Anwendungspool installiert werden soll. Diese Option ermöglicht es, Anwendungen unabhängig voneinander einzustellen. Ist die Option aktiviert, wird jede Anwendung in ihren eigenen Anwendungspool installiert.
Anwendungspool	Anwendungspool, der verwendet werden soll. Die Angabe ist nur möglich, wenn die Option **Dedizierter Anwendungspool einrichten** deaktiviert ist. Wenn Sie den Standardwert **DefaultAppPool** verwenden, wird der Anwendungspool nach folgender Syntax gebildet: `<Anwendungsname>_POOL`
Identität	Berechtigung für die Ausführung des Anwendungspool. Sie können eine Standard-Identität oder ein benutzerdefiniertes Benutzerkonto verwenden. Wenn Sie den Standardwert **ApplicationPoolIdentity** verwenden, wird das Benutzerkonto nach folgender Syntax gebildet: `IIS APPPOOL\<Anwendungsname>_POOL` Wenn Sie einen anderen Benutzer berechtigen möchten, klicken Sie **...** neben dem Eingabefeld, aktivieren Sie die Option **Benutzerdefiniertes Konto** und erfassen Sie den Benutzer und sein Kennwort.
Web-Authentifizierung	Authentifizierungsart gegenüber der Webanwendung. Zur Auswahl stehen: • **Windows Authentifizierung (Single Sign-On)**

Einstellung	Beschreibung
	Der Benutzer wird gegenüber dem Internet Information Services mithilfe seines Windows-Benutzerkontos authentifiziert und die Webanwendung meldet die diesem Benutzerkonto zugeordnete Person rollenbasiert an. Sollte dieses Single Sign-on nicht möglich sein, wird der Benutzer auf eine Anmeldeseite umgeleitet. Diese Authentifizierung ist nur wählbar, wenn die Windows-Authentifizierung installiert ist. • **Anonym** Eine Anmeldung ohne Windows-Authentifizierung ist möglich. Der Benutzer wird gegenüber dem Internet Information Services und der Webanwendung anonym authentifiziert und die Webanmeldung leitet auf eine Anmeldeseite um.
Datenbank-Authentifizierung	HINWEIS: Dieser Bereich wird Ihnen nur angezeigt, wenn Sie auf der Seite **Datenbankverbindung** eine SQL-Datenbankverbindung ausgewählt haben. Authentifizierungsart gegenüber der One Identity Manager-Datenbank. Zur Auswahl stehen: • **Windows Authentifizierung** Die Webanwendung authentifiziert sich gegenüber der One Identity Manager-Datenbank mit dem Windows-Benutzerkonto, unter dem ihr Anwendungspool läuft. Eine Anmeldung ist über ein benutzerdefiniertes Benutzerkonto oder einer Standard-Identität für den Anwendungspool möglich. • **SQL-Authentifizierung** Die Authentifizierung erfolgt mittels SQL Server-Anmeldung und Kennwort. Es wird die SQL Server-Anmeldung aus der Verbindung zur Datenbank verwendet. Über die Schaltfläche [**...**] können Sie eine abweichende SQL-Anmeldung angeben, beispielsweise wenn die Anwendung mit einer Berechtigungsebene für Endbenutzer ausgeführt werden soll. Diese Zugangsdaten werden maschinenspezifisch verschlüsselt in der Konfiguration der Webanwendung gespeichert.

8. Klicken Sie **Weiter**.

   Wenn Sie zuvor eine direkte Datenbankverbindung ausgewählt haben, wird Ihnen die Seite **Anwendungsserver wählen** angezeigt. Die Angabe eines Anwendungsservers ist erforderlich, wenn Sie die Volltextsuche verwenden möchten.

Sie können den Anwendungsserver auch zu einem späteren Zeitpunkt in die Konfigurationsdatei eintragen.

9. (Optional) Auf der Seite **Anwendungsserver wählen** nehmen Sie die folgenden Aktionen vor:

   HINWEIS: Wenn Sie im Web Designer Web Portal die Volltextsuche verwenden möchten, müssen Sie einen Anwendungsserver angeben. Sie können den Anwendungsserver auch zu einem späteren Zeitpunkt in die Konfigurationsdatei eintragen.

   HINWEIS: Wenn Sie die Windows-Authentifizierung verwenden und sich der Anwendungsserver auf einem anderem Host als das Web Designer Web Portal befindet oder falls der Anwendungsserver ein anderes Benutzerkonto für den Anwendungspool als das Web Portal verwendet, müssen Sie in der Active-Directory-Umgebung weitere Einstellungen vornehmen (zum Beispiel, eine Kerberos-Delegierung).

   a. Klicken Sie **Anwendungsserver eintragen**.
   b. Im Dialogfenster im Feld **URL** geben Sie die Adresse des Anwendungsservers ein, auf dem der Suchdienst für die Volltextsuche installiert ist.
   c. Klicken Sie **OK**.

10. Auf der Seite **Anwendungsserver wählen** klicken Sie **Weiter**.
11. Auf der Seite **Installationsziel wählen** nehmen Sie Im Bereich **Installationsquelle** eine der folgenden Aktionen vor:
    - Um die Installationsdaten aus der Datenbank zu beziehen, aktivieren Sie die Option **Aus Datenbank laden**.

      - ODER -

    - Um die Installationsdaten aus dem Installationsmedium (beispielsweise von der Festplatte) zu beziehen, aktivieren Sie die Option **Aus lokalem Ordner installieren** und geben Sie einen Pfad an.
12. In der Auswahlliste **Webprojekt** wählen Sie das gewünschte Webprojekt und geben Sie gegebenenfalls die Authentifizierungsdaten an:

    HINWEIS: Sollten keine weiteren Authentifizierungseinstellungen erforderlich sein, wird Ihnen die Meldung **Keine Authentifizierungsdaten benötigt** angezeigt.

    a. Klicken Sie  .
    b. Im Dialogfenster **Authentifizierungsdaten** klicken Sie auf ein rotes Projekt.
    c. Unter **Authentifizierungsverfahren** geben Sie das Verfahren und die Anmeldedaten an, mit denen Sie sich anmelden möchten.
    d. Führen Sie diese Schritte für alle weiteren roten Projekte durch.
    e. Klicken Sie **OK**.
13. Auf der Seite **Setze das Konto für Aktualisierung** legen Sie das Benutzerkonto für die automatische Aktualisierung fest, indem Sie eine der folgenden Optionen

aktivieren:

HINWEIS: Das Benutzerkonto wird verwendet, um die Dateien im Anwendungsverzeichnis anzulegen oder auszutauschen.

- **Nutze die IIS-Berechtigungen für Aktualisierungen**: Um das Benutzerkonto, unter dem der Anwendungspool ausgeführt wird, für die Aktualisierungen zu nutzen, aktivieren Sie diese Option.
- **Nutze ein spezielles Konto für die Aktualisierungen**: Um ein anderes Benutzerkonto zu verwenden, aktivieren Sie diese Option. Geben Sie die Domäne, den Benutzernamen und das Kennwort des Benutzers an.

14. Klicken Sie **Weiter**.
15. Auf der Seite **Anwendungstoken** geben Sie im Eingabefeld das Anwendungstoken für das Webprojekt ein.

    TIPP: Um ein neues Token zu verwenden und das bestehende Token in der Datenbank zu ersetzen, aktivieren Sie die Option **Ersetze das Anwendungstoken in der Datenbank**. Beachten Sie dabei, dass das bisherig verwendete Token an allen bereits verwendeten Stellen ungültig wird und Sie diese Stellen gegebenenfalls mit dem neuen Token aktualisieren müssen.

    HINWEIS: Behandeln Sie das Anwendungstoken wie ein Passwort. Sobald das Anwendungstoken in der Datenbank gespeichert wird, kann es nicht mehr im Klartext angezeigt werden. Notieren Sie sich das Anwendungstoken gegebenenfalls.
16. Klicken Sie **Weiter**.

    Die Seite **Installation läuft** öffnet sich und zeigt die einzelnen Installationsschritte. Der Web Installer generiert die Webanwendung und die entsprechenden Konfigurationsdateien zu jedem Ordner.
17. Auf der Seite **Installation läuft** werden die einzelnen Installationsschritte angezeigt. Der Web Installer generiert die Webanwendung und die entsprechenden Konfigurationsdateien zu jedem Ordner.
18. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
19. Auf der Seite **Installation prüfen** testen Sie den Start der Webanwendung. Die Basis-URL für den Mailversand wird angezeigt. Wählen Sie gegebenenfalls im Auswahlfeld **Ändern in** eine andere URL.
20. Klicken Sie **Weiter**.
21. Auf der Seite **Beenden des Assistenten** klicken Sie **Fertig**.
22. Schließen Sie das Autorun-Programm.

Verwandte Themen

- Minimale Systemanforderungen für den Webserver auf Seite 42
- Anwendungsserver installieren auf Seite 136
- Web Designer Web Portal konfigurieren auf Seite 159
- Authentifizierungsdaten für die Webanwendung auf Seite 161

Web Designer Web Portal aktualisieren

HINWEIS:

- Es wird empfohlen die automatische Aktualisierung nur in speziellen Wartungsfenstern durchzuführen, in denen die Anwendung von den Benutzern nicht erreichbar ist und der Neustart der Anwendung gefahrlos manuell durchgeführt werden kann.
- Für die automatische Aktualisierung sind folgende Berechtigungen erforderlich:
  - Das Benutzerkonto für die Aktualisierung benötigt die Berechtigung zum Schreiben auf das Anwendungsverzeichnis.
  - Das Benutzerkonto für die Aktualisierung benötigt die lokale Sicherheitsrichtlinie **Anmelden als Stapelverarbeitungsauftrag**.
  - Das Benutzerkonto, unter dem der Anwendungspool läuft, benötigt die lokalen Sicherheitsrichtlinien **Ersetzen eines Tokens auf Prozessebene** und **Anpassen von Speicherkontingenten für einen Prozess**.

Die Konfigurationseinstellungen für die automatische Aktualisierung der Webanwendung nehmen Sie in der Konfigurationsdatei `web.config` vor. Verwenden Sie dazu den Web Designer Configuration Editor.

Um die Webanwendung automatisch zu aktualisieren

1. Öffnen Sie den Runtime Monitor im Browser.
2. Wählen Sie auf dem Tabreiter **Status** eine der Optionen **Jetzt aktualisieren** oder **Aktualisieren, wenn alle Sitzungen beendet sind**.

Um eine Webanwendung manuell zu aktualisieren

- Deinstallieren Sie die bestehende Web Designer Web Portal Installation und installieren Sie das Web Designer Web Portal neu.

Beachten Sie, dass jeder Schreibvorgang auf dem `bin` Ordner der Webanwendung sofort zu einem Neustart der Webanwendung führt. Dies bedeutet, dass alle aktiven Sitzungen auf der Anwendung beendet werden und alle nicht gespeicherten Daten verloren gehen. Aus diesem Grund sollten Sie manuelle Aktualisierungen der Webanwendung nur durchführen, wenn keine aktive Sitzung stattfindet.

Verwandte Themen

- Automatische Aktualisierung für das Web Designer Web Portal konfigurieren auf Seite 164
- Automatische Aktualisierung von Webanwendungen auf Seite 106
- Web Designer Web Portal installieren auf Seite 152
- Runtime Monitor anzeigen auf Seite 167
- Wartungsmodus auf Seite 169

Web Designer Web Portal deinstallieren

Um eine Webanwendung zu deinstallieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:
   a. Wechseln Sie zum Tabreiter **Installation**.
   b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

   Der Web Installer wird gestartet.
3. Auf der Startseite des Web Installer klicken Sie **Deinstallieren einer Webanwendung** und klicken Sie **Weiter**.
4. Auf der Seite **Deinstallieren einer Webanwendung** doppelklicken Sie die Webanwendung, die Sie entfernen möchten.

   Vor der Anwendung wird das Symbol angezeigt.
5. Klicken Sie **Weiter**.
6. Auf der Seite **Datenbankverbindung** wählen Sie die Datenbankverbindung und das Authentifizierungsverfahren und geben Sie die entsprechenden Anmeldedaten ein.
7. Klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installation läuft** werden die einzelnen Schritte zur Deinstallation angezeigt.
10. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
11. Auf der Seite **Beenden des Assistenten** klicken Sie **Fertig**.
12. Schließen Sie das Autorun-Programm.

Web Designer Web Portal konfigurieren

Die Konfiguration des Web Designer Web Portal umfasst eine Reihe von Einstellungen. Die Konfiguration wird in den Konfigurationsdateien `web.config`, `NLog.config` und `monitor.config` der Webanwendung, die sich im Basisverzeichnis der Webanwendung befinden, sowie in der Tabelle `QBMWebApplication` der One Identity Manager-Datenbank gespeichert.

Verwenden Sie den Web Designer Configuration Editor (`WebDesigner.ConfigFileEditor.exe`), um die Konfigurationsdatei `web.config` zu bearbeiten.

Verbindungszeichenfolgen und Anmeldeinformationen werden automatisch in den Konfigurationsdateien mit der Standard MicrosoftASP.NET Kryptographie verschlüsselt.

Um eine Webanwendung zu konfigurieren

1. Starten Sie das Programm `WebDesigner.ConfigFileEditor.exe` aus dem Installationsverzeichnis der Webanwendung.
2. In der Ansicht **Konfigurationsdatei öffnen** wählen Sie die Konfigurationsdatei `web.config` und klicken Sie **Öffnen**.
3. Wählen Sie das erforderlichen Authentifizierungsverfahren und melden Sie sich an.

In den einzelnen Bereichen des Web Designer Configuration Editor nehmen Sie die Konfigurationseinstellungen vor.

Detaillierte Informationen zum Thema

- Datenbankverbindung konfigurieren auf Seite 160
- Authentifizierungsdaten für die Webanwendung auf Seite 161
- Protokollierung zur Webanwendung auf Seite 162
- Automatische Aktualisierung für das Web Designer Web Portal konfigurieren auf Seite 164
- Erweiterte Webeinstellungen auf Seite 165
- Ablage der Cache-Verzeichnisse auf Seite 165
- Debugger Service konfigurieren auf Seite 166
- Suchdienst konfigurieren auf Seite 166

Datenbankverbindung konfigurieren

Die aktuellen Verbindungseinstellungen für das Web Designer Web Portal sehen Sie im Web Designer Configuration Editor im Bereich **Datenbankverbindung**. Bei Bedarf können Sie die Einstellungen anpassen.

Um eine neue Datenbankverbindung auszuwählen

1. Öffnen Sie den Web Designer Configuration Editor.
2. Klicken Sie im Bereich **Datenbankverbindung** den Link **Neue Datenbankverbindung eintragen**.
3. Wählen Sie den Systemtyp erfassen Sie die Verbindungsdaten.
    - Für den Systemtyp **SQL Server** erfassen Sie folgende Informationen.
        - **Server**: Datenbankserver.
        - (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.

- **Nutzer**: SQL Server Anmeldename des Benutzer.
- **Kennwort**: Kennwort für die SQL Server Anmeldung des Benutzer.
- **Datenbank**: Wählen Sie die Datenbank.

- Für den Systemtyp **Anwendungsserver** erfassen Sie die URL.

HINWEIS: Wählen Sie bei Bedarf im Auswahlfeld **Optionen** entweder **Verbindung testen** oder **Erweiterte Optionen**.

Verwandte Themen

- Anmelden an der One Identity Manager-Datenbank auf Seite 179

Authentifizierungsdaten für die Webanwendung

Die Authentifizierungsdaten für das Webprojekt und Subprojekte konfigurieren Sie im Web Designer Configuration Editor im Bereich **Webprojekt**. Ausführliche Informationen zu den Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 30: Authentifizierungsdaten für das Webprojekt

Einstellung	Beschreibung
Webprojekt	Name des Webprojektes.
Authentifizierungsmodul	Authentifizierungsmodul zur Anmeldung am Webprojekt. HINWEIS: Einige Authentifizierungsmodule unterstützen Single Sign-On. In solchen Fällen wird unterhalb des Auswahlfeldes eine Meldung mit entsprechendem Hinweis angezeigt.
Single-Sign-On durchführen, im Fehlerfall Anmeldung über folgendes Modul	Wenn das unter **Authentifizierungsmodul** gewählte Modul Single Sign-On unterstützt, haben Sie hier die Möglichkeit, eine alternative Authentifizierungsmethode anzugeben. Auf diese Authentifizierungsmethode wird zurückgegriffen, wenn eine Single Sign-On Anmeldung auf Grund eines Fehlers nicht möglich sein sollte.
Debugging	Aktivieren Sie die Option, wenn Sie eine Debugging-Umgebung verwenden möchten.
OAuth	Wenn Sie die Authentifzierungsmodule **OAuth 2.0/OpenID Connect** oder **OAuth 2.0/OpenID Connect (rollenbasiert)** verwenden, nehmen Sie hier Konfigurationseinstellungen vor.
OAuth 2.0/OpenID	Wählen Sie die OAuth 2.0/OpenID Connect Konfiguration, die

Einstellung	Beschreibung
Connect Konfiguration	Sie anpassen möchten.
Client-ID für OAuth-Authentifizierung	ID der Anwendung beim Identitätsanbieter. Beispiel: urn:OneIdentityManager/Web
Ausstellerinformationen des OAuth Zertifikates	Wird verwendet, um das Zertifikat im Zertifikatsspeicher zu finden. Es wird entweder der Fingerabdruck oder die Ausstellerinformationen benötigt. Beispiel: `O=[Firmenname], OU=[Organisationseinheit], CN=[IP des Servers]`
OAuth Ressource	Uniform Resource Name (URN) der abzufragenden Ressource. Wird nur benötigt, wenn der Identitätsanbieter diesen Wert erfordert.
Fingerabdruck des OAuth Zertifikates	Fingerabdruck des zu verwendenden Zertifikates zur Prüfung des Sicherheitstokens. Es wird entweder der Fingerabdruck oder die Ausstellerinformationen benötigt.
Endpoint	Uniform Resource Locator (URL) des Zertifikatsendpunkts auf dem Autorisierungsserver. Beispiel: https://certificateServer/certificate.crt
Authentifizierungsdaten für Subprojekte	Authentifizierungsdaten für Subprojekte.

Um Authentifizierungsdaten für ein Subprojekt zu erfassen oder zu ändern

1. Öffnen Sie den Web Designer Configuration Editor.
2. Klicken Sie im Bereich **Webprojekt** neben der Meldung **Authentifizierungsdaten für Subprojekte sind nicht eingetragen** auf die Schaltfläche .
3. Markieren Sie im Bearbeitungsfenster das rot markierte Projekt.
4. Wählen Sie im Bereich **Authentifizierungsverfahren** das gewünschte Authentifizierungsverfahren und erfassen Sie die erforderlichen Anmeldeinformationen.
5. Klicken Sie **OK**.

Protokollierung zur Webanwendung

Die Einstellungen für die Protokollierung zur Webanwendung konfigurieren Sie im Web Designer Configuration Editor im Bereich **Protokoll**. Der Bereich ist unterteilt in:

- Allgemein
- Anwendungsprotokoll

- Ereignisprotokoll
- Datenbankprotokoll

Tabelle 31: Allgemeine Einstellungen für die Protokollierung

Einstellung	Beschreibung
Anwendung	Name der Webanwendung.
Firmennamen	Name des Unternehmens, das die Webanwendung verwendet.
Produktnamen	Produktname des Softwareherstellers
Protokollverzeichnis	Verzeichnis, in dem die Protokolldateien der Webanwendung gespeichert werden. Der Web Server Prozess muss Schreibberechtigungen auf diesen Ordner haben.

Tabelle 32: Einstellungen für das Anwendungsprotokoll

Einstellung	Protokollierung
Schweregrad	Informationsgrad der Protokollierung.
Archivierungsintervall	Maximale Laufzeit einer Protokolldatei, bevor diese umbenannt wird. Hat eine Protokolldatei ihr maximales Alter erreicht, wird die Datei umbenannt und eine neue Protokolldatei wird angefangen.
Nummerierung	Gibt an, ob die Archivdateien des Anwendungsprotokolls aufsteigend oder absteigend nummeriert werden sollen.

Tabelle 33: Einstellungen für das Ereignisprotokoll

Einstellung	Beschreibung
Schweregrad	Informationsgrad der Protokollierung.

Tabelle 34: Einstellungen für das Datenbankprotokoll

Einstellung	Beschreibung
Schweregrad	Informationsgrad der Protokollierung.
Archivierungsintervall	Maximale Laufzeit einer Protokolldatei, bevor diese umbenannt wird. Hat eine Protokolldatei ihr maximales Alter erreicht, wird die Datei umbenannt und eine neue Protokolldatei wird angefangen.
Nummerierung	Gibt an, ob die Archivdateien des Datenbankprotokolls aufsteigend oder absteigend nummeriert werden sollen.

Tabelle 35: Zulässige Schweregrade

Informationsgrad	Beschreibung
Aus	Es werden keine Informationen protokolliert.
Trace	Es erfolgt die Ausgabe sehr ausführlicher Informationen. Diese Einstellung sollte nur zu Analysezwecken verwendet werden. Das Protokoll wird schnell groß und unübersichtlich.
Debug	Es erfolgt die Aufzeichnung von Debugger-Ausgaben. Diese Einstellung sollte nur zu Testzwecken verwendet werden.
Info	Es werden alle Informationen aufgezeichnet.
Warnung	Es werden alle Warnungen aufgezeichnet.
Fehler	Es werden alle Fehlermeldungen aufgezeichnet.
Fatal	Es werden alle kritischen Fehlermeldungen aufgezeichnet.

Automatische Aktualisierung für das Web Designer Web Portal konfigurieren

HINWEIS: Für die automatische Aktualisierung sind folgende Berechtigungen erforderlich:

- Das Benutzerkonto für die Aktualisierung benötigt die Berechtigung zum Schreiben auf das Anwendungsverzeichnis.
- Das Benutzerkonto für die Aktualisierung benötigt die lokale Sicherheitsrichtlinie **Anmelden als Stapelverarbeitungsauftrag**.
- Das Benutzerkonto, unter dem der Anwendungspool läuft, benötigt die lokalen Sicherheitsrichtlinien **Ersetzen eines Tokens auf Prozessebene** und **Anpassen von Speicherkontingenten für einen Prozess**.

Die automatische Aktualisierung konfigurieren Sie im Web Designer Configuration Editor im Bereich **Automatische Aktualisierung**.

Um die automatische Aktualisierung der Webanwendung zu konfigurieren

1. Öffnen Sie den Web Designer Configuration Editor.
2. Aktivieren Sie im Bereich **Automatische Aktualisierung** die Option **Anwendung automatisch aktualisieren**.
3. Legen Sie das Benutzerkonto für die automatische Aktualisierung fest. Das Benutzerkonto wird verwendet, um die Dateien im Anwendungsverzeichnis anzulegen oder auszutauschen.
    - **Nutze die IIS-Berechtigungen für Aktualisierungen**: Um das Benutzerkonto, unter welcher der Anwendungspool ausgeführt wird, für die

Aktualisierungen zu nutzen, aktivieren Sie die Option.

- **Nutze ein spezielles Konto für die Aktualisierungen**: Um ein anderes Benutzerkonto zu verwenden, aktivieren Sie die Option. Geben Sie die Domäne, den Benutzernamen und das Kennwort des Benutzers an.

Verwandte Themen

- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- Automatische Aktualisierung von Webanwendungen auf Seite 106
- Web Designer Web Portal aktualisieren auf Seite 158

Erweiterte Webeinstellungen

Im Bereich **Webeinstellungen** des Web Designer Configuration Editors konfigurieren Sie folgende Webeinstellungen.

Tabelle 36: Webeinstellung

Einstellung	Beschreibung
HTML-Kopfzeilen	HTTP-Kopfzeilen, die der Server bei jeder HTTP-Anfrage ausgibt.
Nach der Abmeldung	Seite, die nach dem Abmelden angezeigt werden soll.
Schließung der Sitzung nach Inaktivität (Min.)	Zeit der Inaktivität nach der die Sitzung geschlossen wird. HINWEIS: Möchten Sie das die Sitzung trotz Inaktivität bestehen bleibt, schreiben Sie in das Eingabefeld den Wert **0**.
HTTP-Übertragung komprimieren	Gibt an, ob die HTTP-Übertragung komprimiert stattfinden soll.
Windows Leistungsindikatoren anlegen	Bei der Installation einer Webanwendung werden grundsätzlich Leistungsindikatoren (PerformanceCounter) registriert, die Auskunft über den Zustand der Anwendung geben. Ausführliche Informationen finden Sie unter Überwachen mithilfe von Leistungsindikatoren auf Seite 169.

Ablage der Cache-Verzeichnisse

Die Ablage der Cache-Verzeichnisse konfigurieren Sie im Web Designer Configuration Editor im Bereich **Cache**.

Tabelle 37: Einstellungen für Cache-Verzeichnisse

Einstellung	Beschreibung
Cache-Verzeichnis	Vollständiger Pfad zum Verzeichnis, in das häufig verwendete Anwendungsinhalte zwischengespeichert werden sollen.
Assembly Cache	Vollständiger Pfad zum Verzeichnis, in das die Assemblies zwischengespeichert werden sollen.

Debugger Service konfigurieren

Für Funktionen der Webanwendung, die den Debugging-Modus unterstützen, muss eine Windows Communication Foundation (WCF) Verbindung hergestellt sein. Den zulässigen Portbereich für die WCF-Verbindung konfigurieren Sie im Web Designer Configuration Editor im Bereich **Debugger Service**.

Um den Portbereich der WCF-Verbindung zu einzugrenzen

1. Öffnen Sie den Web Designer Configuration Editor.
2. Aktivieren Sie im Bereich **Debugger Service** die Option **Portbereich einschränken** und legen Sie die Grenzen für den Port der Verbindung fest.

Suchdienst konfigurieren

Voraussetzung für die Nutzung des Web Designer Web Portal ist ein Anwendungsserver, auf dem der Suchdienst installiert ist.

- Wenn Sie das Web Designer Web Portal direkt über einen Anwendungsserver mit installiertem Suchdienst betreiben, können Sie die Volltextsuche sofort nutzen.
- Wenn Sie das Web Designer Web Portal mit einem Anwendungsserver ohne installierten Suchdienst oder mit einer direkten Datenbankverbindung betreiben, tragen Sie in der Konfiguration der Webanwendung einen Anwendungsserver mit installiertem Suchdienst ein.

  Den Anwendungsserver erfassen Sie in der Regel bei der Web Designer Web Portal Installation. Für die nachträgliche Änderung verwenden Sie den Web Designer Configuration Editor.

Um einen Anwendungsserver nachträglich einzutragen

1. Öffnen Sie den Web Designer Configuration Editor.
2. Klicken Sie im Bereich **Suchdienst** auf **Anwendungsserver eintragen**.
3. Erfassen Sie im Eingabefeld **URL** die Webadresse des Anwendungsservers.

4. Testen Sie die Verbindung über den Eintrag **Verbindung testen** aus dem Kontextmenü **Optionen**.
5. Bearbeiten Sie weitere optionale Einstellungen über den Eintrag **Erweiterte Optionen** aus dem Kontextmenü **Optionen**.
6. Um die Einstellungen zu übernehmen, klicken Sie **OK**.

In der Standardinstallation sind bereits einige wichtige Spalten für die Volltextsuche indiziert. Bei Bedarf können Sie weitere Spalten für die Volltextsuche konfigurieren.

Ausführliche Informationen zur Konfiguration von Spalten für die Volltextsuche finden Sie im *One Identity Manager Konfigurationshandbuch*. Ausführliche Informationen zur Nutzung der Volltextsuche im Web Designer Web Portal finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

Verwandte Themen

- Installieren und Aktualisieren eines Anwendungsservers auf Seite 135
- Web Designer Web Portal installieren auf Seite 152

Wartung des Web Designer Web Portals

Nachfolgend werden Wartungsmöglichkeiten aufgeführt und beschrieben, die für eine Webanwendung zur Verfügung stehen.

Detaillierte Informationen zum Thema

- Runtime Monitor anzeigen auf Seite 167
- Protokolldateien und Exceptions auf Seite 168
- Wartungsmodus auf Seite 169
- Überwachen mithilfe von Leistungsindikatoren auf Seite 169

Runtime Monitor anzeigen

Das Web Designer Web Portal beinhaltet einen Runtime Monitor zur Überwachung. Der Runtime Monitor ist über ein Browserfrontend erreichbar.

Der Aufruf erfolgt mit der entsprechenden URL:

http://<servername>/<application>/monitor

Verwandte Themen

- Zugriffsberechtigungen für den Runtime Monitor auf Seite 168

Zugriffsberechtigungen für den Runtime Monitor

Der Zugriff auf den Runtime Monitor wird in der Konfigurationsdatei (`monitor.config`) der Webanwendung konfiguriert. Die Standardeinstellung erlaubt nur Mitgliedern der Gruppe **BUILTIN\Administrators** auf den Runtime Monitor zuzugreifen.

```
<?xml version="1.0"?>
<!-- Permission to use WebDesigner runtime monitor -->
<authorization>
     <allow roles="BUILTIN\Administrators" />
     <deny users="*" />
</authorization>
```

Für weitere Informationen über das Ändern dieser Einstellung, lesen Sie in der ASP.NET Dokumentation.

Protokolldateien und Exceptions

Die Protokolldateien werden im Runtime Monitor angezeigt.

- Auf dem Tabreiter **Protokolldateien** werden alle Protokolldateien, die von der Webanwendung generiert wurden, angezeigt.

  Sie können diese Dateien filtern und nach Begriffen suchen. Die Protokolldateien befinden sich in physischer Form im Protokollverzeichnis, das durch die Konfiguration in der Konfigurationsdatei der Webanwendung festgelegt wurde, typischerweise `./Logs`).
- Auf dem Tabreiter **Exceptions** werden Protokollmeldungen angezeigt, die Ausnahmefehler enthalten. Diese Meldungen werden nach Ausnahmefehler und absteigender Häufigkeit sortiert. Der oberste Ausnahmefehler in der Liste ist die am häufigsten vorkommende Meldung.

HINWEIS: Der Web Installer schreibt wichtige Ereignisse in die Protokolldatei der Anwendung. Sie können sich diese Protokolldatei in der Windows Ereignisanzeige ansehen.

Verwandte Themen

- Protokollierung zur Webanwendung auf Seite 162
- Runtime Monitor anzeigen auf Seite 167

Wartungsmodus

Um Wartungsarbeiten auszuführen, schalten Sie die Webanwendung in den Wartungsmodus. Nutzen Sie den Wartungsmodus, um beispielsweise eine Aktualisierung zu einem bestimmten Zeitpunkt zu erlauben.

Im Wartungsmodus werden keine neuen Sitzungen zugelassen. Laufende Sitzungen sind nicht betroffen. Benutzern, die sich die Webanwendung ansehen, wird während der Wartung der Inhalt der Datei `Maintenance.html` angezeigt, die sich im Installationsverzeichnis der Webanwendung befindet. Sie können diese Datei bearbeiten, um Details über die Wartungsarbeit für den Benutzer anzuzeigen.

Um die Webanwendung in den Wartungsmodus zu versetzen

1. Öffnen Sie den Runtime Monitor im Browser.
2. Klicken Sie auf dem Tabreiter **Status** die Schaltfläche **Starte Wartungsmodus**.

Um den Wartungsmodus zu beenden

1. Öffnen Sie den Runtime Monitor im Browser.
2. Klicken Sie auf dem Tabreiter **Status** die Schaltfläche **Beende Wartungsmodus**.

Der Wartungsmodus kann auch durch das Anlegen der Datei `App_Data\Maintenance.mode` im Installationsverzeichnis der Webanwendung eingeschaltet und durch ihr Entfernen beendet werden.

Verwandte Themen

- Runtime Monitor anzeigen auf Seite 167

Überwachen mithilfe von Leistungsindikatoren

Bei der Installation einer Webanwendung werden grundsätzlich Leistungsindikatoren registriert, die Auskunft über den Zustand der Anwendung geben.

Eine nachträgliche Installation der Leistungsindikatoren ist möglich.

> HINWEIS: Voraussetzungen hierfür sind, dass die Webanwendung auf einem Windows Server installiert ist und über ausreichende Berechtigungen verfügt, um Leistungsindikatoren anzubieten. Hierfür kann es erforderlich sein, das Benutzerkonto des Anwendungspools in die lokale Gruppe **Leistungsüberwachungsbenutzer** aufzunehmen. Außerdem muss die Webanwendung gestartet sein, um die Leistungsindikatoren auswählen zu können.

Um Leistungsindikatoren nachträglich zu installieren

1. Öffnen Sie den Web Designer Configuration Editor.
2. Klicken Sie auf **Webeinstellungen** und **Windows Leistungsindikatoren anlegen**.

   Nach erfolgreicher Ausführung wird ein Hinweis zur Installation angezeigt.
3. Bestätigen Sie die Hinweismeldung mit **OK**.

Um Leistungsindikatoren einzusehen

1. Melden Sie sich an dem Server an, auf dem die Webanwendung installiert ist.
2. Starten Sie die Leistungsüberwachung von Windows.
3. Wählen Sie im Dialogfenster auf der linken Seite den Eintrag **Leistungsüberwachung**.
4. Klicken Sie im Anzeigebereich der Leistungsüberwachung auf ✚.
5. Markieren Sie im Dialogfenster **Leistungsindikatoren hinzufügen** unter **Verfügbare Leistungsindikatoren** den Eintrag **One Identity ManagerWeb Portal** und erweitern Sie den Eintrag.

   Die Leistungsindikatoren der Webanwendung werden angezeigt. Es stehen folgende Indikatoren zur Verfügung.

   Tabelle 38: Leistungsindikatoren

Leistungsindikator	Beschreibung
AJAX calls	Anzahl der asynchron bearbeiteten HTTP-Anfragen.
Objects	Anzahl der aktiven Datenbankobjekte.
Exceptions	Anzahl der aufgetretenen Ausnahmefehler.
Forms	Anzahl der aktiven Formulare.
HTML requests	Anzahl der HTML-Seitenanfragen.
PID	Anzahl der Prozess-IDs.
Contexts	Anzahl der aktiven Modulobjekte.
Sessions	Anzahl der aktiven Sitzungen.
Sessions total	Gesamtanzahl der Sitzungen seit Anwendungsstart.

6. Fügen Sie die gewünschten Leistungsindikatoren hinzu und wählen Sie unter **Instanzen des ausgewählten Objekts:** Ihre gewünschte Webanwendung aus.

   TIPP: Es werden nur die Webanwendungen zur Auswahl angezeigt, die gestartet sind. Bei der Installation einer neuen Webanwendung, ist es möglich, dass die zur Auswahl stehenden Webanwendungen inklusive der neu installierten Webanwendung erst nach einigen Minuten zur Verfügung stehen.

Installieren und Aktualisieren der Manager Webanwendung

Die Funktionen des Manager können als Webanwendung bereitgestellt werden. Stellen Sie vor der Installation sicher, dass die minimalen Hardware- und Softwarevoraussetzungen auf dem Server erfüllt sind.

Detaillierte Informationen zum Thema

- Minimale Systemanforderungen für den Webserver auf Seite 42
- Manager Webanwendung installieren auf Seite 171
- Manager Webanwendung aktualisieren auf Seite 175
- Manager Webanwendung deinstallieren auf Seite 176
- Erweiterte Konfiguration der Manager Webanwendung auf Seite 198

Manager Webanwendung installieren

Der One Identity Manager erfordert, dass jede Webanwendung auf genau eine Sprache festgelegt wird. Wenn Sie die Anwendung in zwei Sprachen veröffentlichen möchten, dann müssen Sie mindestens zwei separate Anwendungen installieren. Standardmäßig installiert der Web Installer eine Anwendung pro Sprache.

Wenn mehrere Anwendungen gleichzeitig laufen, können Sie einen Sprachen-Pool für diese Anwendungen definieren. Wenn der Benutzer eine Webanwendung des Sprachen-Pools aufruft, wird er automatisch auf die gemäß seiner Sprache passende Webanwendung des Sprachen-Pools umgeleitet. Es ist also nicht nötig, die URLs aller Webanwendungen im Sprachen-Pool bekannt zu machen.

Über diesen Mechanismus lässt sich auch eine einfache Lastverteilung realisieren.

WICHTIG: Starten Sie die Installation der Manager Webanwendung lokal auf dem Server.

Um die Manager Webanwendung zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:
   a. Wechseln Sie zum Tabreiter **Installation**.
   b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

   Der Web Installer wird gestartet.
3. Auf der Startseite des Web Installer wählen Sie **Manager Webanwendung installieren** und klicken Sie **Weiter**.
4. Auf der Seite **Datenbankverbindung** nehmen Sie eine der folgenden Aktionen vor:

   TIPP: Es wird die Verwendung einer Verbindung über einen Anwendungsserver empfohlen.

   - Um eine bestehende Verbindung zur One Identity Manager-Datenbank zu verwenden, wählen Sie in der Auswahlliste **Datenbankverbindung auswählen** die entsprechende Verbindung aus.

     - ODER -

   - Um eine neue Verbindung zur One Identity Manager-Datenbank zu verwenden, klicken Sie **Neue Verbindung erstellen** und geben Sie eine neue Verbindung an.
5. Unter **Authentifizierungsverfahren** geben Sie das Verfahren und die Anmeldedaten an, mit denen Sie sich an der Datenbank anmelden möchten.
6. Auf der Seite **Installationsziel wählen** nehmen Sie die folgenden Einstellungen vor.

Tabelle 39: Einstellungen für das Installationsziel

Einstellung	Beschreibung
Anwendungsname	Name, der als Anwendungsname zum Beispiel in der Titelzeile des Browsers verwendet werden soll.
Zielpfad im IIS	Webseite auf dem Internet Information Services, auf dem die Anwendung installiert wird.
SSL erzwingen	Gibt an, ob sichere oder unsichere Webseiten zur Installation angeboten werden. Ist die Option aktiviert, können nur Seiten, die per SSL gesichert sind, zur Installation verwendet werden. Diese Einstellung ist der Standardwert. Ist die Option nicht aktiviert, können unsichere Webseiten zur Installation verwendet werden.
URL	Uniform Resource Locator (URL) der Anwendung.
Dedizierten Anwen-	Gibt an, ob für jede Anwendung ein eigener Anwendungspool

Einstellung	Beschreibung
dungspool einrichten	installiert werden soll. Diese Option ermöglicht es, Anwendungen unabhängig voneinander einzustellen. Ist die Option aktiviert, wird jede Anwendung in ihren eigenen Anwendungspool installiert.
Anwendungspool	Anwendungspool, der verwendet werden soll. Die Angabe ist nur möglich, wenn die Option **Dedizierter Anwendungspool einrichten** deaktiviert ist. Wenn Sie den Standardwert **DefaultAppPool** verwenden, wird der Anwendungspool nach folgender Syntax gebildet: `<Anwendungsname>_POOL`
Identität	Berechtigung für die Ausführung des Anwendungspool. Sie können eine Standard-Identität oder ein benutzerdefiniertes Benutzerkonto verwenden. Wenn Sie den Standardwert **ApplicationPoolIdentity** verwenden, wird das Benutzerkonto nach folgender Syntax gebildet: `IIS APPPOOL\<Anwendungsname>_POOL` Wenn Sie einen anderen Benutzer berechtigen möchten, klicken Sie **...** neben dem Eingabefeld, aktivieren Sie die Option **Benutzerdefiniertes Konto** und erfassen Sie den Benutzer und sein Kennwort.
Web-Authentifizierung	Authentifizierungsart gegenüber der Webanwendung. Zur Auswahl stehen: • **Windows Authentifizierung (Single Sign-On)** Der Benutzer wird gegenüber dem Internet Information Services mithilfe seines Windows-Benutzerkontos authentifiziert und die Webanwendung meldet die diesem Benutzerkonto zugeordnete Person rollenbasiert an. Sollte dieses Single Sign-on nicht möglich sein, wird der Benutzer auf eine Anmeldeseite umgeleitet. Diese Authentifizierung ist nur wählbar, wenn die Windows-Authentifizierung installiert ist. • **Anonym** Eine Anmeldung ohne Windows-Authentifizierung ist möglich. Der Benutzer wird gegenüber dem Internet Information Services und der Webanwendung anonym authentifiziert und die Webanmeldung leitet auf eine Anmeldeseite um.
Datenbank-Authen-	HINWEIS: Dieser Bereich wird Ihnen nur angezeigt, wenn

Einstellung	Beschreibung
tifizierung	Sie auf der Seite **Datenbankverbindung** eine SQL-Datenbankverbindung ausgewählt haben. Authentifizierungsart gegenüber der One Identity Manager-Datenbank. Zur Auswahl stehen: • **Windows Authentifizierung** Die Webanwendung authentifiziert sich gegenüber der One Identity Manager-Datenbank mit dem Windows-Benutzerkonto, unter dem ihr Anwendungspool läuft. Eine Anmeldung ist über ein benutzerdefiniertes Benutzerkonto oder einer Standard-Identität für den Anwendungspool möglich. • **SQL-Authentifizierung** Die Authentifizierung erfolgt mittels SQL Server-Anmeldung und Kennwort. Es wird die SQL Server-Anmeldung aus der Verbindung zur Datenbank verwendet. Über die Schaltfläche [**...**] können Sie eine abweichende SQL-Anmeldung angeben, beispielsweise wenn die Anwendung mit einer Berechtigungsebene für Endbenutzer ausgeführt werden soll. Diese Zugangsdaten werden maschinenspezifisch verschlüsselt in der Konfiguration der Webanwendung gespeichert.

7. Auf der Seite **Konfiguration** legen Sie weitere anwendungsspezifische Einstellungen fest.
   a. Wählen Sie in der Auswahlliste **Kultur** die Sprachkultur der Anwendung. Die Sprachkultur hat unter anderem Einfluss auf die Darstellung von Datumswerten und sowie Zahlen.
   b. Die Webanwendung benötigt Zugriffsberechtigungen auf sich selbst. Wenn Sie als Authentifizierungsart **Windows-Authentifizierung (Single Sign-On)** für die Web-Authentifizierung gewählt haben, geben Sie Domäne, Benutzerkonto und Kennwort des Benutzers. Bei anonymer Web-Authentifizierung sind keine weiteren Angaben erforderlich.
8. Auf der Seite **Setze das Konto für Aktualisierung** legen Sie das Benutzerkonto für die automatische Aktualisierung fest. Das Benutzerkonto wird verwendet, um die Dateien im Anwendungsverzeichnis anzulegen oder auszutauschen.
   - **Nutze die IIS-Berechtigungen für Aktualisierungen**: Um das Benutzerkonto, unter welcher der Anwendungspool ausgeführt wird, für die Aktualisierungen zu nutzen, aktivieren Sie die Option.
   - **Nutze ein spezielles Konto für die Aktualisierungen**: Um ein anderes

Benutzerkonto zu verwenden, aktivieren Sie die Option. Geben Sie die Domäne, den Benutzernamen und das Kennwort des Benutzers an.

9. Auf der Seite **Installation läuft** werden die einzelnen Installationsschritte angezeigt. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
10. Auf der letzten Seite klicken Sie **Fertig**, um das Programm zu beenden.

HINWEIS: Der Web Installer generiert die Webanwendung und die Konfigurationsdatei (`web.config`). Der Web Installer verwendet Standardwerte für die Konfigurationseinstellungen. Sie können diese Werte beibehalten. Es wird empfohlen, dass Sie die Einstellungen mithilfe des Manager Web Configuration Editor überprüfen. Die Konfigurationsdatei (`web.config`) finden Sie im Verzeichnis der Webanwendung im Internet Information Services.

Verwandte Themen

- Manager Webanwendung aktualisieren auf Seite 175
- Erweiterte Konfiguration der Manager Webanwendung auf Seite 198

Manager Webanwendung anzeigen

Die Manager Webanwendung ist über ein Browserfrontend erreichbar.

Der Aufruf erfolgt mit der entsprechenden URL:

http://<Servername>/<Anwendungsname>

https://<Servername>/<Anwendungsname>

Manager Webanwendung aktualisieren

HINWEIS:

- Es wird empfohlen die automatische Aktualisierung nur in speziellen Wartungsfenstern durchzuführen, in denen die Anwendung von den Benutzern nicht erreichbar ist und der Neustart der Anwendung gefahrlos manuell durchgeführt werden kann.
- Für die automatische Aktualisierung sind folgende Berechtigungen erforderlich:
  - Das Benutzerkonto für die Aktualisierung benötigt die Berechtigung zum Schreiben auf das Anwendungsverzeichnis.
  - Das Benutzerkonto für die Aktualisierung benötigt die lokale Sicherheitsrichtlinie **Anmelden als Stapelverarbeitungsauftrag**.

- Das Benutzerkonto, unter dem der Anwendungspool läuft, benötigt die lokalen Sicherheitsrichtlinien **Ersetzen eines Tokens auf Prozessebene** und **Anpassen von Speicherkontingenten für einen Prozess**.

Die Aktualisierung der Anwendung erfolgt automatisch, wenn das Plugin **Automatische Aktualisierung** für die Webanwendung aktiviert wurde.

Um eine Aktualisierung durchzuführen, sind zunächst die zu aktualisierenden Dateien in die One Identity Manager-Datenbank einzuspielen. Die benötigten Dateien werden beim Einspielen eines Hotfixes, eines Service Packs oder einer Versionsänderung in die One Identity Manager-Datenbank eingefügt und aktualisiert.

Das Plugin **Automatische Aktualisierung** führt eine Prüfung beim Start der Anwendung und danach etwa alle **5** Minuten durch. Werden neue Dateien erkannt, so werden diese aus der Datenbank geladen. Das Plugin kann die Dateien nicht aktualisieren, solange die Anwendung läuft. Die Aktualisierung wartet bis die Anwendung neu gestartet wird.

Der Neustart der Anwendung erfolgt durch den Webserver automatisch, wenn die Anwendung eine definierte Zeitspanne keine Benutzeraktivität aufweist. Dies kann einige Zeit dauern oder durch ununterbrochene Benutzeranfragen verhindert werden.

Verwandte Themen

- Automatisches Aktualisieren des One Identity Manager auf Seite 101
- Erweiterte Konfiguration der Manager Webanwendung auf Seite 198

Manager Webanwendung deinstallieren

Um eine Webanwendung zu deinstallieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Auf der Startseite des Installationsassistenten:
   a. Wechseln Sie zum Tabreiter **Installation**.
   b. Im Bereich **Web-basierte Komponenten** klicken Sie **Installieren**.

   Der Web Installer wird gestartet.
3. Auf der Startseite des Web Installer klicken Sie **Deinstallieren einer Webanwendung** und klicken Sie **Weiter**.
4. Auf der Seite **Deinstallieren einer Webanwendung** doppelklicken Sie die Webanwendung, die Sie entfernen möchten.

   Vor der Anwendung wird das Symbol angezeigt.
5. Klicken Sie **Weiter**.
6. Auf der Seite **Datenbankverbindung** wählen Sie die Datenbankverbindung und das Authentifizierungsverfahren und geben Sie die entsprechenden Anmeldedaten ein.

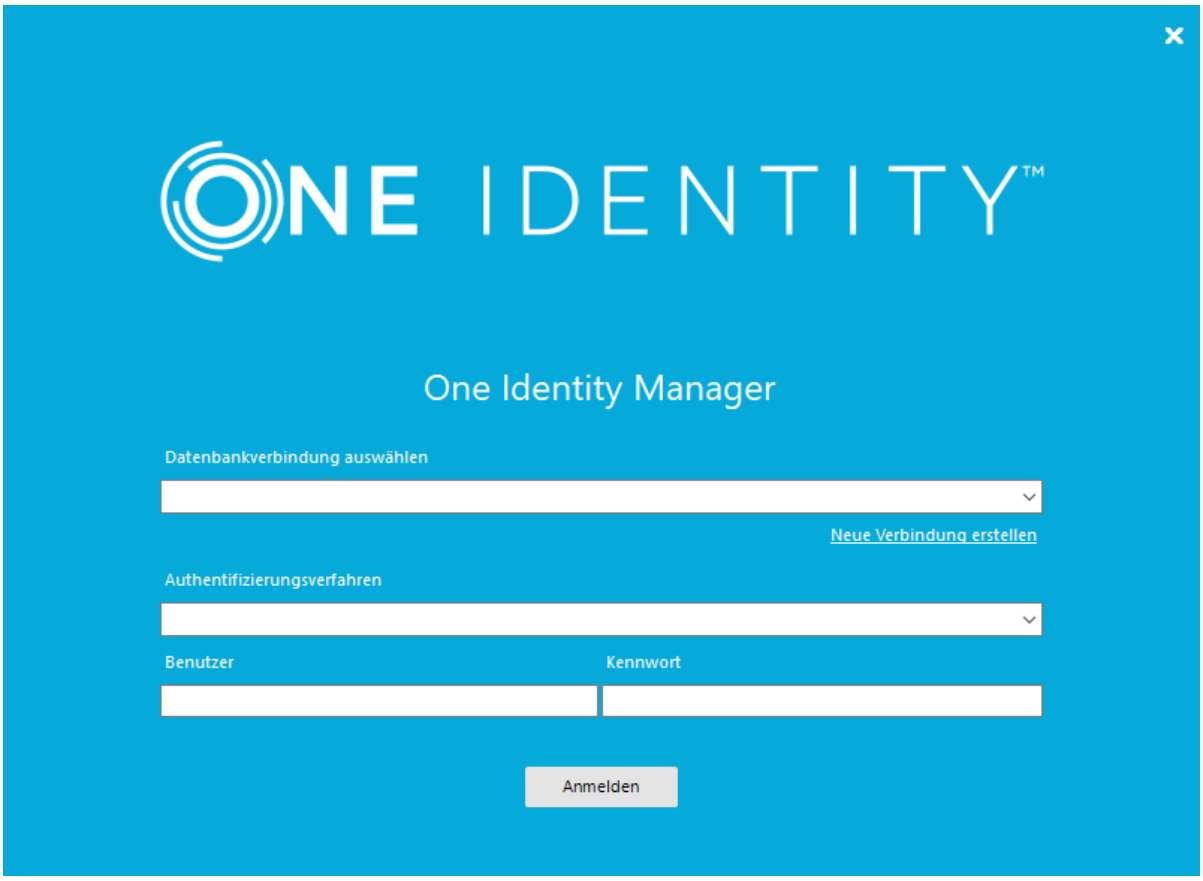
7. Klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installation läuft** werden die einzelnen Schritte zur Deinstallation angezeigt.
10. Nachdem der Installationsvorgang abgeschlossen wurde, klicken Sie **Weiter**.
11. Auf der Seite **Beenden des Assistenten** klicken Sie **Fertig**.
12. Schließen Sie das Autorun-Programm.

Anmelden an den One Identity Manager-Werkzeugen

HINWEIS: Das Starten der One Identity Manager-Werkzeuge ist nur zulässig, wenn der Benutzer die entsprechenden Programmfunktionen besitzt. Ausführliche Informationen zu den Programmfunktionen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Beim Starten eines One Identity Manager-Werkzeugs wird der Standardverbindungsdialog geöffnet. Es wird versucht die zuletzt verwendete Verbindung wiederherzustellen.

Abbildung 5: Standardverbindungsdialog



Bei der Anmeldung wird zwischen dem Benutzer der Datenbank und dem Benutzer der einzelnen One Identity Manager-Werkzeuge (Systembenutzer) unterschieden. Es können mehrere Systembenutzer mit einem Datenbankbenutzer arbeiten.

Die Anmeldung erfolgt in zwei Schritten:

1. Auswählen der Datenbankverbindung zur Anmeldung an der Datenbank

   Die Anmeldung an der Datenbank kann über einen Anwendungsserver oder eine direkte Verbindung zur Datenbank erfolgen.

2. Auswählen des Authentifizierungsverfahrens und des Systembenutzers für die Anmeldung

   Die zulässigen Systembenutzerkennungen werden über das eingesetzte Authentifizierungsmodul ermittelt. Der One Identity Manager stellt dafür verschiedene Authentifizierungsmodule zur Verfügung.

   HINWEIS: Nach der initialen Schemainstallation sind im One Identity Manager nur die Authentifizierungsmodule **Systembenutzer** und **ComponentAuthenticator** sowie die rollenbasierten Authentifizierungsmodule aktiviert. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

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

Detaillierte Informationen zum Thema

- Anmelden an der One Identity Manager-Datenbank auf Seite 179
- Anmelden an den One Identity Manager-Werkzeugen mit einer Systembenutzerkennung auf Seite 182
- Weitere Authentifizierungsmodule aktivieren auf Seite 183
- Weitere Anmeldesprachen aktivieren auf Seite 185
- Überprüfung der Authentifizierung auf Seite 186
- Ablauf von Kennwörtern auf Seite 185

Anmelden an der One Identity Manager-Datenbank

Um eine vorhandene Verbindung auszuwählen

- Wählen Sie im Verbindungsdialog die Verbindung unter **Datenbankverbindung auswählen**.

HINWEIS:

- Neu erstellte Verbindungen werden erst nach erneutem Start des Programms im Verbindungsdialog angezeigt.
- Verbindungen, die nicht die erwartete Berechtigungsebene für SQL Server Anmeldungen verwenden, werden nicht im Verbindungsdialog angezeigt.
- Die Berechtigungsebene für eine vorhandene Verbindung wird im Tooltipp für die Auswahlliste angezeigt.

  Ausführliche Informationen zu den minimalen Berechtigungsebenen der One Identity Manager-Werkzeuge finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Um eine neue Verbindung zur One Identity Manager-Datenbank zu erstellen

1. Klicken Sie unter **Datenbankverbindung auswählen** auf **Neue Verbindung erstellen** und wählen Sie den Systemtyp **SQL Server**.
2. Klicken Sie **Weiter**.
3. Erfassen Sie die Verbindungsdaten zum Datenbankserver.
   - **Server**: Datenbankserver.
   - (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
   - **Nutzer**: SQL Server Anmeldename des Benutzer.
   - **Kennwort**: Kennwort für die SQL Server Anmeldung des Benutzer.
   - **Datenbank**: Wählen Sie die Datenbank.
4. Wählen Sie über die Schaltfläche **Optionen** den Eintrag **Verbindung testen**.

   Es wird versucht die Datenbankverbindung mit den angegebenen Verbindungsdaten aufzubauen. Es wird eine Meldung zum Test ausgegeben, die Sie bestätigen.

   HINWEIS: Über den Eintrag **Optionen > Erweiterte Optionen** können Sie weitere Konfigurationseinstellungen für die Verbindung vornehmen.
5. Klicken Sie **Fertig**.

Um eine neue Verbindung zum Anwendungsserver herzustellen

1. Klicken Sie unter **Datenbankverbindung auswählen** auf **Neue Verbindung erstellen** und wählen Sie den Systemtyp **Anwendungsserver**.
2. Klicken Sie **Weiter**.
3. Erfassen Sie die Adresse (URL) zum Anwendungsserver.
4. Wenn Sie auf einen per SSL/TLS gesicherten Anwendungsserver zugreifen, konfigurieren Sie zusätzliche Einstellungen zum Zertifikat.

- Stimmen Servername des Zertifikats und die Adresse (URL) zum Anwendungsserver überein und konnte das Serverzertifikat erfolgreich geprüft werden, wird der Servername neben dem Eingabefeld für die URL grün hinterlegt. Per Klick auf den Servernamen neben dem Eingabefeld für die URL können Sie Informationen zum Zertifikat anzeigen.
- Stimmen Servername des Zertifikats und die Adresse (URL) zum Anwendungsserver nicht überein oder konnte das Serverzertifikat erfolgreich geprüft werden, wird der Servername neben dem Eingabefeld für die URL rot hinterlegt. Legen Sie fest, ob Sie dem Zertifikat vertrauen.
- Wird laut SSL Einstellungen ein Clientzertifikat erwartet, wählen Sie unter **Clientzertifikat festlegen**, das Zertifikat aus und legen Sie fest, wie das Zertifikat geprüft werden soll. Zur Auswahl stehen **Nach Antragsteller suchen**, **Nach Herausgeber suchen** und **Nach Fingerabdruck suchen**.
- Wenn Sie mit einem selbstsignierten Zertifikat zugreifen wollen, aktivieren Sie die Option **Akzeptiere selbstsigniertes Zertifikat**.

5. Wählen Sie über die Schaltfläche **Optionen** den Eintrag **Verbindung testen**.

   Es wird versucht die Datenbankverbindung mit den angegebenen Verbindungsdaten aufzubauen. Es wird eine Meldung zum Test ausgegeben, die Sie bestätigen.

   HINWEIS: Über den Eintrag **Optionen > Erweiterte Optionen** können Sie weitere Konfigurationseinstellungen für die Verbindung vornehmen.

6. Klicken Sie **Fertig**.

Um eine Verbindung zu löschen

1. Wählen Sie unter **Datenbankverbindung auswählen** die Verbindung.
2. Drücken Sie **Entf**.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die ausgewählte Datenbankverbindung wird nun nicht mehr im Verbindungsdialog angezeigt.

Um einen SQL Server aus der Serverliste zu löschen

1. Klicken Sie unter **Datenbankverbindung auswählen** auf **Neue Verbindung erstellen** und wählen Sie den Systemtyp **SQL Server**.
2. Klicken Sie **Weiter**.
3. Öffnen Sie Auswahlliste **Server** und markieren Sie den Server, den Sie löschen möchten.
4. Drücken Sie die Taste **Entf**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Der SQL Server wird nun nicht mehr zur Auswahl angeboten.

Verwandte Themen

- Anmelden an den One Identity Manager-Werkzeugen mit einer Systembenutzerkennung auf Seite 182

Anmelden an den One Identity Manager-Werkzeugen mit einer Systembenutzerkennung

Im Anschluss an die Datenbankanmeldung meldet sich der Benutzer mit einer Systembenutzerkennung am gestarteten Programm an. Die zulässigen Systembenutzerkennungen werden über das eingesetzte Authentifizierungsmodul ermittelt.

HINWEIS:

- Nach der initialen Schemainstallation sind im One Identity Manager nur die Authentifizierungsmodule **Systembenutzer** und **ComponentAuthenticator** sowie die rollenbasierten Authentifizierungsmodule aktiviert.
- Das Starten der One Identity Manager-Werkzeuge ist nur zulässig, wenn der Benutzer die entsprechenden Programmfunktionen besitzt.
- Für die Anmeldung am Designer verwenden Sie nicht-rollenbasierte Authentifizierungsmodule. Rollenbasierte Authentifizierungsmodule werden für die Anmeldung am Designer nicht unterstützt.

Um sich an den One Identity Manager Werkzeugen mit einer Systembenutzerkennung anzumelden

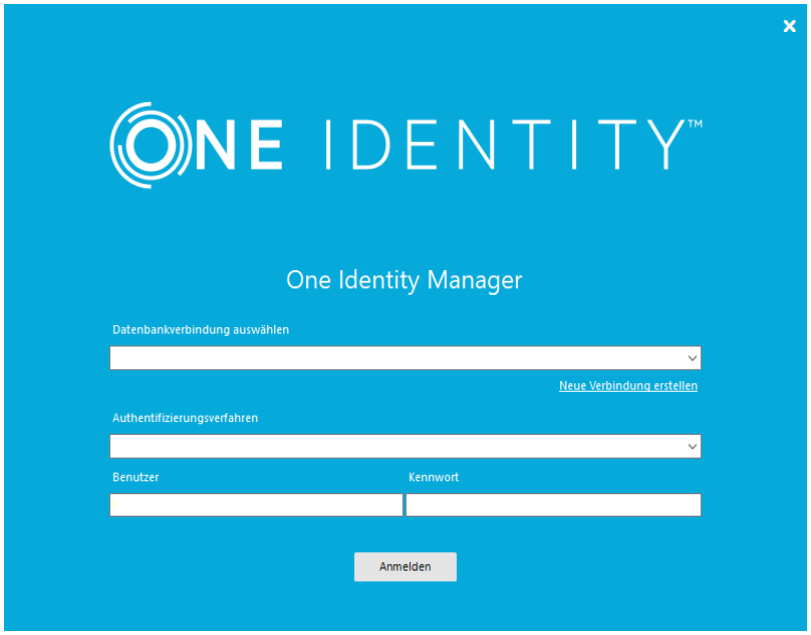
1. Wählen Sie im Verbindungsdialog unter **Authentifizierungsverfahren** das Authentifizierungsmodul.

   Es wird eine Auswahlliste eingeblendet, die alle freigeschalteten Authentifizierungsmodule enthält.
2. Erfassen Sie die Anmeldedaten für die Systembenutzerkennung.

   Die Anmeldedaten sind abhängig vom gewählten Authentifizierungsmodul.
3. Klicken Sie **Anmelden**.

   Die Verbindungsdaten werden gespeichert und stehen bei der nächsten Anmeldung zur Verfügung.

Abbildung 6: Anmeldefenster



Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen und zu den Programmfunktionen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Verwandte Themen

- Anmelden an der One Identity Manager-Datenbank auf Seite 179
- Weitere Authentifizierungsmodule aktivieren auf Seite 183
- Fehlermeldungen bei der Anmeldung an den One Identity Manager-Werkzeugen auf Seite 189

Weitere Authentifizierungsmodule aktivieren

Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

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**.

Spracheinstellungen des One Identity Manager

Die Standardinstallation des One Identity Manager wird in den Sprachen **English - United States [en-US]** und **German - Germany [de-DE]** ausgeliefert. Bei Bedarf können Sie weitere Sprachen zur Gestaltung der Benutzeroberfläche und der Ausgabetexte einpflegen. Für diesen Fall müssen Sie vor Einsatz des One Identity Manager die verwendeten Texte in die neue Sprache übersetzen. Für die Übersetzung steht Ihnen im Designer einen Wörterbucheditor zur Verfügung. In den One Identity Manager-Werkzeugen wird die Eingabe mehrsprachiger Inhalte durch ein spezielles Steuerelement unterstützt.

Standardsprache des One Identity Manager

Die Stammdatenpflege erfolgt immer in der Standardsprache. Die Standardsprache einer One Identity Manager-Installation ist **English - United States [en-US]**. Die Standardsprache ist systemweit gültig. Eine Änderung der Standardsprache im laufenden Betrieb wird nicht empfohlen.

Im Idealfall stimmen Standardsprache des One Identity Manager und die Anmeldesprache der Benutzer an den Administrationswerkzeugen überein. Unterscheiden sich die Anmeldesprache des Benutzers und die Standardsprache, so wird die Standardsprache dann verwendet, wenn bei einer sprachabhängigen Datenauflösung für die angeforderte Anmeldesprache des Benutzers keine übersetzten Bezeichnungen gefunden werden.

Anmeldesprache des Benutzers

Die Darstellung der Anzeigetexte in der Benutzeroberfläche erfolgt in der Sprache, mit der sich ein Benutzer an den Administrationswerkzeugen anmeldet. Bei der erstmaligen Anmeldung an den Werkzeugen wird die Systemsprache zur Anzeige der Benutzeroberfläche verwendet. Der Benutzer kann seine Anmeldesprache in jedem Administrationswerkzeug in den Programmeinstellungen ändern. Dabei wird die Anmeldesprache global für alle Werkzeuge, mit denen der Benutzer arbeitet, festgelegt. Somit muss die Einstellung der Anmeldesprache nicht in jedem Werkzeug erneut erfolgen. Die Änderung der Anmeldesprache wird erst mit dem Neustart der Werkzeuge wirksam.

Als Anmeldesprachen werden alle Sprachen angeboten, für die die Option **Wählbar im Frontend** aktiviert ist.

Verwandte Themen

- Weitere Anmeldesprachen aktivieren auf Seite 185

Weitere Anmeldesprachen aktivieren

Als Anmeldesprachen werden alle Sprachen angeboten, für die die Option **Wählbar im Frontend** aktiviert ist.

Um weitere Anmeldesprachen zu aktivieren

1. Wählen Sie im Designer die Kategorie **Basisdaten > Lokalisierung > Sprachkulturen**.
2. Wählen Sie im Listeneditor die Sprache.
3. Setzen Sie in der Ansicht **Eigenschaften** die Eigenschaft **Wählbar im Frontend** auf den Wert **True**.
4. Speichern Sie die Änderungen.
5. Wählen Sie den Menüeintrag **Datenbank > Übertragung in Datenbank** und klicken Sie **Speichern**.

Verwandte Themen

- Spracheinstellungen des One Identity Manager auf Seite 184

Ablauf von Kennwörtern

Um einen Benutzer darüber zu informieren, dass sein Kennwort abläuft, werden verschiedene Funktionen eingesetzt:

- Bei der Anmeldung am One Identity Manager wird der Benutzer auf ein ablaufendes Kennwort hingewiesen und kann sein Kennwort gegebenenfalls ändern.
- Das System verschickt für Personen-basierte Authentifizierungsmodule Erinnerungsbenachrichtigungen zu ablaufenden Kennwörtern ab 7 Tage vor dem Ablauf des Kennwortes.
    - Die Zeit in Tagen können Sie im Konfigurationsparameter **Common | Authentication | DialogUserPasswordReminder** anpassen. Bearbeiten Sie den Konfigurationsparameter im Designer.

- Die Benachrichtigungen werden nach dem Zeitplan **Erinnerung Ablauf des Systembenutzerkennwortes** ausgelöst und verwenden die Mailvorlage **Person-Systembenutzerkennwort läuft ab**. Den Zeitplan und die Mailvorlage können Sie bei Bedarf im Designer anpassen.

TIPP: 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`).

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.

Verbindungspool für getrennte Sitzungen für Lesen und Schreiben auf verschiedenen Datenbankservern

Um getrennte Sitzungen für Lesen und Schreiben auf verschiedenen Datenbankservern zu nutzen, passen Sie in den Verbindungsdaten die Eigenschaft **Data Source** an.

Die Eigenschaft **Data Source** kann eine Pipe (|) getrennte Serverliste enthalten. Dabei ist der erste angegebene Server der primäre Server, über den die Schreibzugriffe laufen. Alle anderen Server sind Read-Only-Kopien, die nur Lesezugriffe erhalten. Voraussetzung ist dabei, dass der Datenbankname und die Anmeldedaten auf den sekundären Servern identisch zum primären Server sind.

HINWEIS: Im Verbindungsdialog erreichen Sie die Eigenschaft über den Eintrag **Optionen > Erweiterte Optionen**

Die internen physischen Sitzungen zum Lesen werden dabei auf die R/O-Kopien und den primären Server zufällig verteilt. Bei einem primären Server und zwei sekundären Servern erhält der primäre Server ungefähr 1/3 der Verbindungen für Leseoperationen.

HINWEIS: Durch den Verbindungspool wird nicht für jede Operation eine neue Verbindung geöffnet. Wenn keine neuen parallelen Anfragen kommen, laufen alle Anfragen über dieselbe Verbindung und damit auf demselben Server.

Das Verfahren darauf angewiesen, dass eine Replikation zwischen den Servern stattfindet und die Daten immer aktuell auch in den Kopien vorliegen.

Verwandte Themen

- Anmelden an der One Identity Manager-Datenbank auf Seite 179

Anhang A

Fehlerbehebung

Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.

Transporthistorie anzeigen und One Identity Manager Version prüfen

Bei einer Schemainstallation oder Schemaaktualisierung mit dem Configuration Wizard werden das Migrationsdatum und der Migrationsstand in der Transporthistorie der Datenbank aufgezeichnet.

Beim Importieren eines Transportpaketes mit dem Database Transporter werden das Datum des Imports, die Beschreibung des Imports, der Versionsstand der Datenbank, der Name des Transportpaketes in der Transporthistorie der Zieldatenbank aufgezeichnet.

Um die Transporthistorie anzuzeigen

- Starten Sie den Designer und wählen Sie das Menü **Hilfe > Transporthistorie**.

Um einen Überblick über die Systemkonfiguration zu erhalten

- Starten Sie den Designer oder den Manager und wählen Sie das Menü **Hilfe > Info**.

  Auf dem Tabreiter **Systeminformationen** erhalten Sie einen Überblick über Ihre aktuelle Systemkonfiguration und die installierten Module mit ihren Versionen.

  WICHTIG: Stellen Sie diese Informationen bereit, wenn Sie den Support kontaktieren.

  HINWEIS: Wenn Sie die Lieferantenbenachrichtigung aktiviert haben, wird dieser Bericht einmal im Monat an One Identity gesendet.

Verwandte Themen

- Lieferantenbenachrichtigung im One Identity Manager auf Seite 78

Fehlermeldungen bei der Anmeldung an den One Identity Manager-Werkzeugen

Problem

Bei der Anmeldung an einem One Identity Manager- Werkzeug erscheint folgende Fehlermeldung:

```
[810284] Der Benutzer konnte nicht authentifiziert werden.
[810015] Die Anmeldung des Benutzers xyz ist gescheitert.
[810017] Falscher Benutzername oder falsches Kennwort.
```

Mögliche Ursachen

- Der angegebene Benutzer wird durch das gewählte Authentifizierungsmodul nicht unterstützt.
- Das angegebene Kennwort ist falsch.
- Der Benutzer, der zur Anmeldung verwendet wird, ist gesperrt.
- Die Person, die zur Anmeldung verwendet wird, ist temporär oder dauerhaft deaktiviert.
- Die Person, die zur Anmeldung verwendet wird, ist als sicherheitsgefährdend eingestuft.

Mögliche Lösungen

- Prüfen Sie die Anmeldeinformationen.
- Prüfen Sie, ob die Person, die zur Anmeldung verwendet wird, gesperrt ist. Nutzen Sie im Manager in der Kategorie **Personen** die folgenden Menüeinträge.
  - **Inaktive Personen**: Es werden die zeitweilig deaktivierten Personen und die dauerhaft deaktivierten Personen angezeigt.
  - **Sicherheitsvorfälle**: Es werden die Personen angezeigt, die als sicherheitsgefährdend eingestuft sind.
  - **Gesperrte Personen**: Es werden die Personen angezeigt, die die Anzahl der maximalen Fehlanmeldungen überschritten haben und somit gesperrt sind.
- Prüfen Sie, ob der Systembenutzer, der zur Anmeldung verwendet wird, gesperrt ist. Gesperrte Systembenutzer werden im Designer in der Kategorie **Berechtigungen > Systembenutzer > Gesperrte Systembenutzer** angezeigt.

Ausführliche Informationen zu deaktivierten Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul.*

Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Damit werden die Personen und Systembenutzer wieder entsperrt. Ausführliche Informationen finden Sie im *One Identity*

Manager Web Designer Web Portal Anwenderhandbuch und im *One Identity Manager Konfigurationshandbuch für Webanwendungen*.

Problem

Bei der Anmeldung an einem One Identity Manager-Werkzeug erscheint folgende Fehlermeldung:

```
[810374] Sie dürfen diese Anwendung nicht ausführen.
```

Ursache

Das Starten der One Identity Manager-Werkzeuge ist nur zulässig, wenn der Benutzer die entsprechenden Programmfunktionen besitzt. Sie verwenden zur Anmeldung eine Systembenutzerkennung, die nicht die Berechtigung zum Starten des Programms besitzt.

Mögliche Lösungen

- Verwenden Sie eine Systembenutzerkennung, die die benötigte Programmfunktion zum Starten des Programms benötigt.
- Stellen Sie dem Systembenutzer die Programmfunktion zur Verfügung.
    - Prüfen Sie im Designer in der Kategorie **Berechtigungen > Programmfunktionen**, welche Berechtigungsgruppe die erforderliche Programmfunktion besitzt.
    - 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 besitzt.

Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen, zu Berechtigungsgruppen und Anwendungsrollen sowie zu den Programmfunktionen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Fehlermeldungen bei der Installation und der Aktualisierung der One Identity Manager-Datenbank

Bevor die Installation oder Aktualisierung der One Identity Manager-Datenbank startet, prüft der Configuration Wizard die Einstellungen des Datenbankservers und der Datenbank, die für die Installation und den Betrieb der One Identity Manager-Datenbank erforderlich sind. Weitere Informationen finden Sie unter Einstellungen für den Datenbankserver und die One Identity Manager-Datenbank auf einem SQL Server auf Seite 25.

Einige dieser Einstellungen werden durch den Configuration Wizard korrigiert. Ist die Korrektur nicht möglich, wird eine entsprechende Meldung im Configuration Wizard ausgegeben. Korrigieren Sie in diesem Fall die Fehler manuell.

Tabelle 40: Meldungen im Configuration Wizard vor dem Start der Installation oder der Aktualisierung einer Datenbank

Meldung	Lösung
Das Datenbanksortierschema stimmt nicht. 'SQL_Latin1_General_CP1_CI_AS' muss konfiguriert sein.	Setzen Sie die Datenbankeigenschaft **Sortierung** (Collation) auf den Wert **SQL_Latin1_General_CP1_CI_AS**.
Die Migration kann nicht ausgeführt werden, da gerade eine Replikation ausgeführt wird.	Weitere Informationen finden Sie unter Datenbankfehler bei der Migration einer Datenbank in SQL Server AlwaysOn-Verfügbarkeitsgruppen auf Seite 193.
Der Wert in 'DialogDatabase.DataOrigin' ist ungültig. Führen Sie erst eine Datenbankkompilierung durch.	Verwenden Sie den Database Compiler, um die Datenbank-ID neu zu erzeugen und die Datenbank zu kompilieren. Es müssen alle Anteile der Datenbank neu kompiliert werden. Achten Sie darauf, dass alle Skriptausdrücke und alle Prozesse zur Kompilierung gekennzeichnet sind.
Die Datenbank besitzt keine Datendateigruppe für In-Memory-OLTP.	Verwenden Sie die Reparaturmethode um eine Datendateigruppe zu erstellen.
Die Datenbank hat keine Datei in der Datendateigruppe für In-Memory-OLTP definiert.	Verwenden Sie die Reparaturmethode um eine Datenbankdatei zu erstellen. Die Datei wird im Verzeichnis der Datendatei (`*.mdf`) erstellt.
Der SQL Server hat In-Memory-OLTP nicht aktiviert.	Setzen Sie die Datenbankservereigenschaft **Extreme Transaktionsverarbeitung unterstützt** (Is XTP Supported) auf den Wert **True**.
Die Datenbankeigenschaft 'Abbruch bei arithmetischem Fehler aktiviert (Arithmetic Abort enabled)' ist nicht aktiviert.	Setzen Sie die Datenbankeigenschaft **Abbruch bei arithmetischem Fehler aktiviert** (Arithmetic Abort enabled) auf den Wert **True**.
Die Datenbankeigenschaft 'Bezeichner in Anführungszeichen aktiviert (Quoted Identifiers Enabled)' ist nicht aktiviert.	Setzen Sie die Datenbankeigenschaft **Bezeichner in Anführungszeichen aktiviert** (Quoted Identifiers Enabled) auf den Wert **True**.
Eine Migration kann nicht ausgeführt werden, wenn das Wiederherstellungsmodel	Setzen Sie die Datenbankeigenschaft **Wiederherstellungsmodell** (Recovery model) auf den Wert **Einfach** (simple).

Meldung	Lösung
nicht 'Einfach (Simple)' ist.	
Der Transaktionsmodus kann nicht gesetzt werden, da andere Benutzer aktiv sind.	Beenden Sie die Verbindungen anderer Benutzer zur Datenbank.
Die Jobqueue und / oder die DBQueue ist nicht leer. In der Dokumentation erhalten Sie weitere Informationen und Lösungsvorschläge zu dieser Prüfung.	Stellen Sie sicher, dass die Prozesse in der Jobqueue und die Aufträge in der DBQueue vor dem Start der Aktualisierung verarbeitet wurden. Verwenden Sie Job Queue Info zur Überwachung der Prozessverarbeitung. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*. Der Configuration Wizard bietet eine Möglichkeit, diese Meldung zu ignorieren. Verwenden Sie diese Möglichkeit nur in Testumgebungen oder Entwicklungsumgebungen. Durch die Aktualisierung der Datenbank können Änderungen erfolgen, die dazu führen, dass die Prozesse anschließend nicht mehr verarbeitet werden können.
Der Systembenutzer 'viadmin' muss ein gültiges und nicht leeres Kennwort haben.	Stellen Sie sicher, dass der Systembenutzer ein gültiges Kennwort besitzt.
Die Datenbank befindet sich im Status 'Initialmigration'. Der Configuration Wizard kann dadurch nicht ausgeführt werden.	Die initiale Schemainstallation der Datenbank wurde nicht vollständig abgeschlossen. Dies kann unterschiedliche Ursachen haben, beispielsweise nicht erreichbarer Datenbankserver oder Clusterschwenks während der Schemainstallation. Erstellen Sie ein neue Datenbank und führen Sie erneut eine initiale Schemainstallation aus. Weitere Informationen finden Sie unter Installieren und Konfigurieren einer One Identity Manager-Datenbank auf Seite 58.
Die SQL Server Anmeldung, welche in QBMDBPrincipal.LoginName angegeben ist, existiert nicht.	Verwenden Sie die Reparaturmethode um die SQL Server Anmeldung zu erstellen.

Datenbankfehler bei der Migration einer Datenbank in SQL Server AlwaysOn-Verfügbarkeitsgruppen

Mögliche Probleme

- Die Aktualisierung der Datenbank startet nicht. Der Configuration Wizard zeigt die Meldung:

  `Die Migration kann nicht ausgeführt werden, da gerade eine Replikation ausgeführt wird.`

- Während der Aktualisierung des One Identity Manager Schemas tritt folgende Fehlermeldung auf:

  `Database error 1468: The operation cannot be performed on database "<database name>" because it is involved in a database mirroring session or an availability group. Some operations are not allowed on a database that is participating in a database mirroring session or in an availability group. ALTER DATABASE statement failed.`

Ursache

Die Datenbank ist Bestandteil einer AlwaysOn-Verfügbarkeitsgruppe.

Lösung

1. Entfernen Sie die Datenbank aus der AlwaysOn-Verfügbarkeitsgruppe.
2. Aktualisieren Sie das One Identity Manager Schema.
3. Nehmen Sie die Datenbank wieder in die AlwaysOn-Verfügbarkeitsgruppe auf.

Meldung: Enter email address in configuration parameter

Die Parameter `SenderAddress` oder `Address` in einem Prozess zum Versenden von E-Mail Benachrichtigungen enthalten den Wert `<Enter email address in configuration parameter "...">`. Die Parameter eines Prozesses prüfen Sie im Job Queue Info.

Ist für den One Identity Manager Service die erweiterte Fehlerausgabe im Debugmodus eingerichtet, wird die Meldung zusätzlich in der Protokolldatei des One Identity Manager Service ausgegeben.

Wahrscheinliches Problem

Der One Identity Manager versendet bei verschiedenen Aktionen im System E-Mail-Benachrichtigungen. Das E-Mail Benachrichtigungssystem des One Identity Manager ist nicht vollständig konfiguriert.

Lösung

Prüfen Sie die Konfigurationsparameter für das E-Mail Benachrichtigungssystem. Nutzen Sie dazu den E-Mail-Konfigurationsassistenten.

Um den E-Mail-Konfigurationsassistenten im Launchpad zu starten

1. Wählen Sie im Launchpad im Bereich **Konfigurieren** den Eintrag **E-Mail-Versand konfigurieren**.
2. Klicken Sie **Starten**.

Um den E-Mail-Konfigurationsassistenten im Designer zu starten

1. Wählen Sie im Designer in der Kategorie **Basisdaten > Allgemein > Konfigurationsparameter** den Konfigurationsparameter **Common | MailNotification**.
2. Klicken Sie im Konfigurationsparametereditor **...** hinter dem Eingabefeld **Wert**.

Detaillierte Informationen zum Thema

- Einrichten des E-Mail-Benachrichtigungssystems auf Seite 81

Nicht benötigte Module aus der One Identity Manager-Datenbank entfernen

Module, die Sie nicht mehr in Ihrer Umgebung benötigen, können Sie aus der One Identity Manager-Datenbank entfernen.

WICHTIG:

- Mit dem Entfernen eines Moduls gehen die Daten dieses Moduls verloren. Erstellen Sie daher vor dem Entfernen eines Moduls eine Sicherung der One Identity Manager-Datenbank.
- Mit dem Entfernen eines Moduls werden unter Umständen Abhängigkeiten zu anderen Modulen entfernt. Daher muss nach dem Entfernen eines Moduls das One Identity Manager Schema aktualisiert werden.
- Nach dem Entfernen eines Moduls können zusätzliche Tests erforderlich sein. Entfernen Sie ein Modul zunächst in Ihrer Testumgebung und testen Sie die Funktion des One Identity Manager ausführlich. Berücksichtigen Sie dabei auch

eventuell vorhandene kundenspezifische Anpassungen, die sich auf Funktionen der entfernten Module beziehen.

Um ein Modul zu entfernen

1. Beenden Sie alle Webanwendungen im Internetinformationsdienste (IIS)-Manager.
2. Beenden Sie alle One Identity Manager-Werkzeuge außer Job Queue Info.
3. Warten Sie bis alle Prozesse beendet sind. Verwenden Sie dazu Job Queue Info.
4. Beenden Sie alle One Identity Manager Services über die Dienstverwaltung.
5. Beenden Sie die Anwendungsserver im IIS-Manager.
6. Warten Sie bis alle DBQueue Prozessor Aufträge beendet sind. Verwenden Sie dazu Job Queue Info.
7. Beenden Sie Job Queue Info.
8. Starten Sie ein geeignetes Programm zur Ausführung von SQL Abfragen.

   WICHTIG:

   - Verwenden Sie für die Ausführung der SQL Abfragen den Benutzer, den Sie auch für die Migration der Datenbank verwenden.
   - Führen Sie die nachfolgenden Schritte einzeln in einem geeigneten Programm zur Ausführung von SQL Abfragen aus.

     Prüfen Sie nach jedem Schritt die Ausgaben der Abfragen. Die Ausgaben geben zusätzliche Hinweise zum Entfernen eines Moduls.

   a. Setzen Sie den Einzelbenutzermodus für die One Identity Manager-Datenbank.

      ```
      exec dbo.QBM_PSingleUserRequest @@spid
      ```

   b. Stoppen Sie die DBQueue Prozessor Komponenten.

      ```
      exec QBM_PWatchDogPrepare 1
      go
      exec QBM_PDBQueuePrepare 1
      go
      ```

   c. Löschen Sie alle Trigger in der Datenbank.

      ```
      exec QBM_PTriggerDrop '%', @force = 1
      ```

   d. Löschen Sie alle Contraints in der Datenbank.

      ```
      exec QBM_PConstraintFKDrop '%','%','%'
      ```

   e. Löschen Sie die nicht mehr benötigten Module.

      ```
      exec QBM_PModuleRemove '<3-stelliges Modulkürzel>'
      ```

      Beispiel:

      ```
      declare @ModulesToRemove varchar(100) = 'SAP' + char(7)
      ```

```
      + 'SHR' + char(7)
      + 'SBW' + char(7)
      + 'SAC' + char(7)
exec QBM_PModuleRemove @ModulesToRemove
go
```

   f. Wenn Sie das Geschäftsrollenmodul (RMB) löschen, müssen Sie zusätzlich Einträge aus der Tabelle `OrgRoot` löschen.

      ```
      exec QBM_PDeleteDeep '<Key><T>OrgRoot</T><P>3031e9af-6a53-4876-bbfb-0f7fbf264131</P></Key>
      ```

9. Beenden Sie den Einzelbenutzermodus für die One Identity Manager-Datenbank.

   ```
   exec dbo.QBM_PSingleUserRelease @@spid
   ```

10. Aktualisieren Sie das One Identity Manager Schema mit dem Configuration Wizard. Wählen Sie alle verbleibenden Module zur Aktualisierung aus.
11. Falls Sie nachträglich Hotfixes vom Support für die Version erhalten haben, müssen Sie diese Hotfixes ebenfalls erneut installieren.
12. Starten Sie den Anwendungsserver, die One Identity Manager Services und die Webanwendungen.

One Identity Manager-Datenbank löschen

Der Configuration Wizard unterstützt Sie beim Löschen einer One Identity Manager-Datenbank. Beim Löschen einer Datenbank werden ebenfalls die Datenbankbenutzer, die Datenbankrollen und Serverrollen sowie die SQL Server Anmeldungen entfernt.

HINWEIS: Starten Sie den Configuration Wizard auf einer administrativen Arbeitsstation.

Um eine Datenbank zu löschen

1. Starten Sie den Configuration Wizard.
2. Auf der Startseite des Configuration Wizard wählen Sie die Option **One Identity Manager-Datenbank löschen** und klicken Sie **Weiter**.
3. Auf der Seite **Datenbank auswählen** wählen Sie Datenbank und das Installationsverzeichnis.
   a. Wählen Sie im Bereich **Datenbankverbindung auswählen** die Datenbankverbindung. Verwenden Sie einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.

b. Wählen Sie im Bereich **Installationsquellen** das Verzeichnis mit den Installationsdateien.

4. Auf der Seite **Datenbanküberprüfung** werden Fehler angezeigt, die eine Verarbeitung der Datenbank verhindern. Beheben Sie die Fehler bevor Sie mit der Aktualisierung fortfahren.
5. Um den Löschvorgang zu starten, klicken Sie **Weiter**.
6. Auf der Seite **Verarbeitung der Datenbank** werden die einzelnen Schritte zum Löschen der Datenbank angezeigt.
   a. Lesen und prüfen Sie die Schritte.
   b. Um die Schritte auszuführen, klicken Sie **Löschen bestätigen**.
   c. Nachdem der Löschvorgang abgeschlossen ist, klicken Sie **Weiter**.
7. Auf der letzten Seite des Configuration Wizard klicken Sie **Fertig**.

Meldungen zur Indizierung des Suchindex

Protokollmeldungen zur Indizierung werden im Protokoll des Anwendungsservers (Standard `\App_Data\Logs\AppServer.log`) ausgegeben.

Im Regelfall wird nach dem Indizierungsintervall laut Konfigurationsparameter **Common | Indexing | Interval** ein neuer Indizierungslauf gestartet.

Wenn eine Indizierung in einer Tabelle mehr als im Konfigurationsparameter **Common | Indexing | BatchSize** angegebene, zu indizierende Objekte vorfindet, wird die Indizierung der Tabelle unterbrochen.

Im Protokoll des Anwendungsservers wird eine Meldung ausgegeben.

```
INFO (Indexing ): Index for Person partially updated, will continue at
next run
```

Sofern mindestens eine Tabelle noch nicht vollständig indiziert wurde, wird die Indizierung nach 3 Sekunden neu gestartet. Im Protokoll des Anwendungsservers wird eine Meldung ausgegeben.

```
INFO (Indexing ): Index is incomplete (28.06%); indexing will continue
in 3000 ms
```

Wenn bereits ein Signal zur Wiederverwendung (`<recycling>`) des Anwendungspools empfangen wurde, lautet die Protokollmeldung beispielsweise:

```
INFO (Indexing ): Index is incomplete (28.06%); indexing will continue when
the application re-starts
```

Solange mindestens eine unvollständige Tabelle vorhanden ist, werden in einem Lauf nur die unvollständigen Tabellen indiziert.

Anhang B

Erweiterte Konfiguration der Manager Webanwendung

HINWEIS: Der Web Installer verwendet Standardwerte für die meisten Konfigurationseinstellungen. Meistens können Sie diese Werte beibehalten. Es wird empfohlen, dass Sie die Einstellungen mithilfe des Manager Web Configuration Editor überprüfen.

Die Konfiguration der Manager Webanwendung erfolgt mit Hilfe des Manager Web Configuration Editor. Der Manager Web Configuration Editor ist Teil der Webanwendung und befindet sich im Installationsverzeichnis im Unterverzeichnis `WebConfigEditor`.

Um die Konfiguration durchzuführen

1. Starten Sie die Datei `WebConfigEditor.exe` und melden Sie sich an der One Identity Manager-Datenbank an.

   Der Manager Web Configuration Editor öffnet automatisch die Datei `web.config` der Webanwendung.
2. Passen Sie die Konfigurationseinstellungen an.
3. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Lastverteilung der Manager Webanwendung auf Seite 207
- Manager Webanwendung Single Sign-On auf Seite 208

Allgemeine Einstellungen der Manager Webanwendung

Im Bereich **Allgemein** des Manager Web Configuration Editors konfigurieren Sie das Erscheinungsbild der Manager Webanwendung.

Tabelle 41: Bedeutung der allgemeinen Konfigurationseinstellungen

Einstellung	Beschreibung
Kultur	Sprache. Die Sprache hat unter anderem Einfluss auf die Darstellung von Datumswerten und Zahlen.
Sitzungs-Timeout	Zeit der Inaktivität eines Benutzers in Minuten, nachdem der Benutzer automatisch abgemeldet werden soll. Dieser Wert ist abhängig vom Timeout-Modus und hat direkten Einfluss auf den Speicherverbrauch und somit auf die Anwendungsperformance. HINWEIS: Dieser Wert sollte so lang wie nötig und so kurz wie möglich gewählt werden, da verwaiste Sitzungen Speicher verbrauchen und die Anwendungsperformance negativ beeinflussen.
Timeout-Modus	Verfahren zur Timeout-Bestimmung. Zulässige Werte sind: • **TimeOut**: Eine Sitzung wird beendet, wenn die unter Sitzungs-Timeout definierte Zeitspanne ohne Aktivität des Benutzers verstrichen ist. • **HeartBeat**: Eine Sitzung wird beendet, wenn die unter Sitzungs-Timeout definierte Zeitspanne ohne Aktivität des Benutzers verstrichen ist. Das offene Browserfenster des Benutzers meldet sich automatisch. So dass der Timeout erst mit dem Schließen des Browserfensters beginnt.
Visualisierung	Visualisierung der Anwendung.
Dynamische Designauswahl	Wird momentan nicht verwendet.
Portalmodus aktivieren	Erlaubt der Anwendung in einem Frame einer anderen Anwendung verlinkt zu werden.

Datenbankverbindung für die Manager Webanwendung

Im Bereich **Datenbankverbindung** des Manager Web Configuration Editors legen Sie alle Datenbankparameter für die Manager Webanwendung fest.

Tabelle 42: Bedeutung der Konfigurationseinstellungen für die Datenbankverbindung

Einstellung	Beschreibung
Datenbank	Datenbankverbindung. Sie können zwischen einer SQL Server Datenbankverbindung und einem Anwendungsserver wählen.
Anwendung	Anwendung, die den Inhalt der Webanwendung festlegt. In der Regel sollten Sie **Manager** wählen.
Anzeigename	Name, der als Anwendungsname zum Beispiel in der Titelzeile des Browsers verwendet werden soll.
Authentifizierung	Verfahren, mit dem die Benutzer bei der Anmeldung an der Anwendung authentifiziert werden sollen.
Schnelle Anmeldung (Single Sign-On)	Gibt an, ob Single Sign-On zur Anmeldung verwendet werden soll. Aktivieren Sie diese Option, wenn Sie Single Sign-On benutzen. Die Anwendung zeigt dadurch keine Anmeldeseite dem Benutzer und versucht dessen Identität automatisch zu ermitteln.

Sicherheitseinstellungen der Manager Webanwendung

Im Bereich **Sicherheit** des Manager Web Configuration Editors legen Sie einige wichtige, die Sicherheit der Manager Webanwendung beeinflussende, Einstellungen fest.

Tabelle 43: Bedeutung der Konfigurationseinstellungen für die Sicherheit

Einstellung	Beschreibung
Installationsumgebung	Standardkonfigurationen der Installationsumgebung. Diese Einstellung wirkt sich auf andere Konfigurationsgruppen aus. Zulässige Werte sind: • **Production**: Empfohlene Einstellung für alle produktiven Installationen. • **Test**: Einstellung, wenn die Anwendung zu Testzwecken

Einstellung	Beschreibung
	installiert wurde. • **Development**: Einstellungen, wenn die Anwendung in einem Entwicklungsumfeld installiert wurde. • **Custom**: Einstellungen, wenn Sie alle Einstellungen manuell vornehmen möchten.
Antwortverzögerung bei ungültiger Sitzung	Zeit in Sekunden, die eine clientseitige Anfrage mit falschen Sitzungsinformationen blockiert werden soll. Diese Einstellung soll eventuelle "Brute Force" Angriffe verhindern.
Anmeldung ohne Cookies erlauben	Die Anwendung nutzt Sitzungs-Cookies zur Sicherung der Client-Server Kommunikation. Aktivieren Sie diese Einstellung, um Benutzeranmeldungen ohne Cookies zu erlauben. Dies wäre der Fall, falls beispielsweise Cookies im Firmennetzwerk verboten wurden. HINWEIS: Es ist empfohlen diese Einstellung nicht zu aktivieren.
Browserfenster nach dem Abmelden schließen	Gibt an, ob das Browserfenster nach Abmeldung geschlossen werden soll. Ist diese Einstellung aktiviert, versucht die Anwendung das Browserfenster des Benutzers zu schließen, nachdem sich dieser abgemeldet hat. Diese Funktion wird nicht von jedem Browser unterstützt oder erfolgt nur nach Nachfrage des Browsers.

HINWEIS: Im Standard ist die Verwendung von SSL deaktiviert. Die Verwendung von SSL kann jetzt optional eingeschaltet werden. Dazu ist in der Konfigurationsdatei der Manager Webanwendung (`Web.config`) in der Sektion `application` folgender Eintrag einzufügen.

```
<add key="AllowSSL" value="True" />
```

Debugging-Einstellungen der Manager Webanwendung

Im Bereich **Debugging** des Manager Web Configuration Editors befinden sich nützliche Einstellungen zur Fehlersuche in der Manager Webanwendung. Im Normalfall müssen Sie hier nichts konfigurieren.

Tabelle 44: Bedeutung der Konfigurationseinstellungen für das Debugging

Einstellung	Beschreibung
Protokollumfang	Menge an Informationen, die protokolliert werden sollen.

Einstellung	Beschreibung
	HINWEIS: Im produktiven Betrieb der Anwendung sollte **Normal** eingestellt werden.
Dokumentationsmodus aktivieren	Gibt an, ob in der Anwendungsoberfläche einige zusätzliche Informationen angezeigt werden, beispielsweise der Name des aktiven Formulars. Die Wirkung ist abhängig von der ausgewählten Visualisierung. HINWEIS: Diese Einstellung sollte im produktiven Betrieb nicht aktiviert werden.
SQL Protokoll aktivieren	Gibt an, ob alle Datenbankanweisungen protokolliert werden sollen. Das Protokoll wird in das SQL Protokollverzeichnis geschrieben. HINWEIS: Diese Einstellung sollte im produktiven Betrieb nicht aktiviert werden.
ASP.Net Fehlermeldungen anzeigen	Gibt an, ob ASP.Net eigene Fehlermeldungen angezeigt werden sollen. HINWEIS: Diese Einstellung sollte im produktiven Betrieb nicht aktiviert werden.
Testmodus aktivieren	Gibt an, ob automatische Tests unterstützt werden sollen. HINWEIS: Diese Einstellung sollte im produktiven Betrieb nicht aktiviert werden.

Verwandte Themen

- Verzeichnisse der Manager Webanwendung konfigurieren auf Seite 204

Leistungseinstellungen der Manager Webanwendung

Im Bereich **Leistung** des Manager Web Configuration Editors legen Sie einige wichtige Einstellungen fest, die die Leistung der Manager Webanwendung beeinflussen.

Tabelle 45: Bedeutung der Konfigurationseinstellungen für die Leistung

Einstellung	Beschreibung
Lastverteilung	Modus der integrierten Lastverteilung. In den meisten Fällen sollte **DistributeEqually** gewählt werden.
Maximale Auslastung	Maximale Anzahl von Benutzersitzungen, die die Anwendung akzeptieren soll. Soll eine große Anzahl von Sitzungen ermöglicht werden, so

Einstellung	Beschreibung
	sollte die Anwendung eventuell mehrfach installiert werden, da die Systemressourcen für jeden Anwendungsprozess limitiert sind.
Maximum erzwingen	Wird diese Einstellung deaktiviert, so wird der Wert unter **Maximale Auslastung** unwirksam. Er wird jedoch als Schwellwert für das Lastverteilungsverfahren **DistributeSuccessively** verwendet.
HTTP-Übertragung komprimieren	Gibt an, ob die Nutzung der Kompression der HTTP Kommunikation aktiviert werden soll. HINWEIS: Die Kompression der HTTP Kommunikation muss auch für den Internet Information Services konfiguriert worden sein. Weitere Informationen finden Sie in der Dokumentation des Webservers.
Host Segmentation	Angabe von Host Segmenten. Die Einstellung ermöglicht die Verteilung der clientseitigen Anfragen auf mehrere Serveradressen die alle Aliase für das Webfrontend darstellen. Damit lassen sich einige Limitierungen des Browsers umgehen und so bei schlechten Netzverbindungen die Ladezeiten verkürzen.

Verwandte Themen

- Lastverteilung der Manager Webanwendung auf Seite 207

Einstellungen zum Dateidownload der Manager Webanwendung

Um den Download größerer Dateien zu ermöglichen, benötigt die Manager Webanwendung ein Verzeichnis in dem der Download dem Benutzer zur Verfügung gestellt werden kann. Dies betrifft zum Beispiel Berichte die von der Anwendung generiert und dann vom Benutzer als PDF gespeichert werden. Die Einstellungen bearbeiten Sie im Bereich **Dateidownload** des Manager Web Configuration Editors.

Tabelle 46: Bedeutung der Konfigurationseinstellungen für den Download von Dateien

Einstellung	Beschreibung
Dateidownload aktivieren	Gibt an, ob Dateidownload aktiviert werden soll. Aktivieren Sie diese Einstellung, um den Download von größeren Dateien, wie Berichten, zu ermöglichen. Ist der Dateidownload deaktiviert, stehen einige Funktionen nicht zur Verfügung.
Downloadverzeichnis	Verzeichnis, das die Anwendung nutzen soll, um die Downloads zur Verfügung zu stellen. Die Anwendung benötigt vollständige

Einstellung	Beschreibung
	Berechtigungen in diesem Verzeichnis.
Säuberungsintervall	Zeitdauer in Minuten, in der nicht benötigten Datei gesucht und entfernt werden.
Bereitstellungsdauer	Zeitdauer in Minuten, in der ein Download dem Benutzer zur Verfügung gestellt werden soll. Nach der Initiierung eines Downloads kann die Anwendung nicht mehr feststellen, wann und ob der Download vom Benutzer durchgeführt wurde, sodass der Download nach einer bestimmten Zeit abgebrochen werden muss.

ASP.Net Basiseinstellungen für die Manager Webanwendung

Im Bereich **ASP.NET Basiseinstellungen** sehen Sie einige Einstellungen des ASP.Net, die Sie mit dem Manager Web Configuration Editor bearbeiten können.

Tabelle 47: Bedeutung der Konfigurationseinstellungen für ASP.Net

Einstellung	Beschreibung
Maximale Anfragelänge	Maximale Größe einer Benutzeranfrage in Kilobyte (kByte). Diese limitiert unter anderem die maximale Größe der Dateien, die hochgeladen werden können.
Maximale Ausführungszeit	Maximale Zeit in Sekunden, die eine Benutzerabfrage bearbeitet werden darf. Das Überschreiten dieser Zeit hat einen harten Abbruch der Benutzeranfrage zur Folge. HINWEIS: Diese Zeit sollte nicht zu kurz festgelegt werden, da das Überschreiten dieser Zeit einen Sitzungsverlust des Benutzers zur Folge haben kann.

Verzeichnisse der Manager Webanwendung konfigurieren

Im Bereich **Verzeichnisse** des Manager Web Configuration Editors konfigurieren Sie alle Verzeichnisse, die die Manager Webanwendung benötigt.

Tabelle 48: Bedeutung der Konfigurationseinstellungen für Verzeichnisse

Einstellung	Beschreibung
Applikationsverzeichnis	Vollständiger Pfad zum Installationsverzeichnis der Anwendung. Dies ist das Verzeichnis indem sich die Datei `web.config` befindet. HINWEIS: Achten Sie auf korrekte Groß-/Kleinschreibung.
Protokollverzeichnis	Verzeichnis, in welches das Anwendungsprotokoll geschrieben werden soll. Dieses Verzeichnis kann relativ zum Applikationsverzeichnis angegeben werden.
Datenbank Cache	Vollständiger Pfad zum Verzeichnis, in das häufig verwendete Datenbankinhalte zwischengespeichert werden sollen.
Skriptassembly Cache	Vollständiger Pfad zum Verzeichnis, in das die Assemblies zwischengespeichert werden sollen.
SQL Protokollverzeichnis	Vollständiger Pfad zum Verzeichnis, in das die Datenbankzugriffe protokolliert werden sollen. Das SQL Protokoll ist nur zur Fehlersuche zu verwenden und muss im Bereich **Debugging** über die Option **SQL Protokoll aktivieren** aktiviert werden.

Verwandte Themen

- Debugging-Einstellungen der Manager Webanwendung auf Seite 201

Applikationspool der Manager Webanwendung konfigurieren

Im Bereich **Applikationspool** des Manager Web Configuration Editors definieren Sie alle Anwendungen die zusammenarbeiten, um die Anwendung dem Benutzer in mehreren Sprachen zur Verfügung zu stellen.

- Klicken Sie auf **Applikation hinzufügen**, um eine weitere Anwendung zu definieren.
- Klicken Sie auf **Applikation entfernen**, um die selektierte Anwendung zu entfernen.
- Mit den beiden Pfeilen auf der rechten Seite können Sie die Reihenfolge ändern.

HINWEIS: Es muss mindestens die aktuell konfigurierte Anwendung definiert werden. Die Reihenfolge hat direkten Einfluss auf die Anmeldeperformance, da der Status der konfigurierten Anwendungen in der definierten Reihenfolge abgefragt wird.

Tabelle 49: Bedeutung der Konfigurationseinstellungen für den Applikationspool

Einstellung	Beschreibung
URL für Weiterleitung	Vollständige Adresse zur Anwendung. Diese Adresse muss auch clientseitig durch die Browser der Benutzer auflösbar sein. HINWEIS: Achten Sie auf korrekte Groß-/Kleinschreibung.
Authentifizierung	Die Anwendungen kommunizieren über die definierte URL untereinander. Dafür werden Berechtigungen benötigt, wenn der anonyme Zugriff nicht erlaubt ist. Die Anwendung benötigt dafür die gleichen Berechtigungen, die auch benötigt werden, wenn die URL per Browser auf dem Server aufgerufen werden soll.

Verwandte Themen

- Lastverteilung der Manager Webanwendung auf Seite 207

Plugins der Manager Webanwendung

Plugins erweitern die Funktionalität der Manager Webanwendung. Sie können ein Plugin aktivieren, indem Sie die Option vor dem Namen des Plugins aktivieren. Unterhalb eines Plugins finden Sie eventuell einige pluginspezifische Einstellungen. Die Einstellungen bearbeiten Sie im Bereich **Plugins** des Manager Web Configuration Editors.

Plugin Automatische Aktualisierung

Dieses Plugin führt die automatische Aktualisierung durch.

Tabelle 50: Bedeutung der Konfigurationseinstellungen

Einstellung	Bedeutung
Automatische Aktualisierung	Die automatische Aktualisierung wird aktiviert.
Schweregrad	Schweregrad einer Änderung, damit die automatische Aktualisierung gestartet wird.

Verwandte Themen

- Manager Webanwendung aktualisieren auf Seite 175
- Automatisches Aktualisieren des One Identity Manager auf Seite 101

Lastverteilung der Manager Webanwendung

Die Manager Webanwendung stellt eine einfache Lastverteilung zur Verfügung, um die Benutzersitzungen und damit auch die entstehende Last auf mehrere Prozesse oder gar Server zu verteilen. Dazu muss die Anwendung mehrfach auf demselben oder auf weiteren Servern installiert werden.

Alle zusammenarbeitenden Anwendungen werden im Applikationspool der Anwendungen bekanntgegeben, auf denen eine Anmeldung möglich sein soll. Der ausgewählte Algorithmus zur Lastverteilung verteilt Benutzeranmeldungen auf die definierten Anwendungen.

HINWEIS: Auch wenn nur eine Anwendung installiert wird, muss diese in ihrem eigenen Applikationspool definiert werden, da sonst keine Anmeldung möglich ist.

Tabelle 51: Unterstützte Algorithmen für die Lastverteilung

Algorithmus	Beschreibung
DistributeEqually	Dieser Algorithmus verteilt die Benutzeranmeldungen so, dass jede Anwendung einer Sprache möglichst die gleiche Anzahl von aktiven Benutzern besitzt. Dieser Algorithmus ist der Standard und wird in 99% der Fälle benötigt.
DistributeSuccessively	Dieser Algorithmus verteilt die Benutzeranmeldungen nach der Definitionsreihenfolge der Anwendungen im Applikationspool. Zuerst werden alle Benutzeranmeldungen auf die erste Anwendung der gewünschten Sprache weitergeleitet. Erst wenn diese ihre maximale Auslastung erreicht hat, werden die Anmeldungen auf die nächste Anwendung weitergeleitet.

Die Lastverteilung löst folgende Probleme:

- Mehrsprachigkeit

  Die Sprache wird pro Anwendung festgelegt, so dass eine Anwendung immer nur Benutzersitzungen in einer Sprache zur Verfügung stellen kann. Sollen Benutzer sich mit mehreren Sprachen anmelden können, so muss für jede Sprache mindestens eine Anwendung installiert werden.

- Umgehung von Ressourcenlimitierungen

  Werden mehrere Webanwendungen installiert und diese unterschiedlichen Internet Information Services Anwendungspools zugewiesen, so werden diese in separaten Prozessen gestartet.

- Performancesteigerung

  Durch die Installation auf mehreren Servern lässt sich die Performance erheblich steigern.

- Redundanz

Durch die mehrfache Installation bedeutet der Ausfall einer installierten Anwendung nicht zwingend den Ausfall des gesamten Verbundes.

Verwandte Themen

- Applikationspool der Manager Webanwendung konfigurieren auf Seite 205

Manager Webanwendung Single Sign-On

Die Manager Webanwendung unterstützt einen Single Sign-On Mechanismus, der es ermöglicht einen Benutzer zu authentifizieren, ohne dass dieser sich erneut per Benutzername und Kennwort authentifizieren muss.

Notwendige Voraussetzungen sind:

- Deaktivierung des anonymen Zugriffs.
- Die Konfiguration eines Single Sign-on fähigen Authentifizierungsmoduls.

  Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
- Berechtigung in dem anwendungseigenen Anwendungspool.

Die Deaktivierung des anonymen Zugriffs erfolgt auf dem Webserver. Dadurch wird der Browser des Benutzers gezwungen die für die Authentifizierung benötigten Informationen zu übermitteln.

Um den anonymen Zugriff zu deaktivieren

1. Öffnen Sie dazu die Konfiguration der Manager Webanwendung in den Internet Information Services und aktivieren Sie die Konfiguration zur **Authentication**.
2. Ändern Sie den Wert für Status bei **Anonymous Authentication** auf **disabled**.

Verwandte Themen

- Applikationspool der Manager Webanwendung konfigurieren auf Seite 205

Anhang C

Maschinenrollen und Installationspakete

Tabelle 52: Mögliche Maschinenrollen und zugehörige Installationspakete

Maschinenrolle	Beschreibung zum Installationspaket
Database Agent	Enthält das Programm `DatabaseAgentServiceCmd.exe` zur Ausführung des Database Agent Service über die Kommandozeile.
Documentation	Enthält die One Identity Manager-Dokumentation in verschiedenen Sprachen.
SCIM Provider	Enthält das SCIM Plugin für den API Server.
Server	Enthält alle Basiskomponenten zur Einrichtung eines Servers.
Server | Jobserver	Enthält den One Identity Manager Service und die Basisprozesskomponenten. Zusätzliche Maschinenrollen enthalten die Konnektoren zur Synchronisation der einzelnen Zielsysteme.
Server | Jobserver | Configuration tool	Enthält die Konfigurationswerkzeuge für den One Identity Manager Service.
Server | Web	Enthält die Basiskomponenten zur Einrichtung eines Webservers.
Server | Web | Application Server	Enthält die Komponenten zur Einrichtung eines Anwendungsservers. Die Maschinenrollen **Search Service** und **Search Indexing Service** werden für die Suchindizierung für die Volltextsuche benötigt. Diese Maschinenrollen sind immer gemeinsam zu verwenden.
Server | Web | Business API Server	Enthält die Komponenten zur Einrichtung eines API Servers.
Server | Web | Manager Web Application	Enthält die Werkzeuge zur Installation und Konfiguration des Manager auf einem Webserver.

Maschinenrolle	Beschreibung zum Installationspaket
Server | Web| End User Web Application	Enthält die Werkzeuge zur Installation und Konfiguration des Web Portal auf einem Webserver.
Workstation	Enthält alle Basiskomponenten zur Installation der Werkzeuge auf einer administrativen Arbeitsstation.
Workstation | Administration	Enthält die Administrationswerkzeuge, die ein Standardbenutzer zur Erfüllung seiner Aufgaben mit dem One Identity Manager benötigt. Neben den Werkzeugen, welche die Grundfunktionalität für die Arbeit mit One Identity Manager sicherstellen, zählt dazu auch der Manager als zentrales Administrationswerkzeug.
Workstation | Commandline administration tools	Enthält verschiedene Kommandozeilenprogramme.
Workstation | Configuration	Enthält alle Werkzeuge des Standardbenutzers und zusätzliche Programme, welche zur Konfiguration des Systems erforderlich sind. Dazu gehören beispielsweise Configuration Wizard, Database Compiler, Database Transporter, Crypto Configuration, Designer, Web Designer sowie Konfigurationswerkzeuge für den One Identity Manager Service.
Workstation | Development & Testing	Enthält die Werkzeuge zur Entwicklung und zum Testen kundenspezifischer Skripte, wie beispielsweise System Debugger.
Workstation | Monitoring	Enthält Programme zur Überwachung des Systemstatus, wie beispielsweise Job Queue Info.

Anhang D

Konfigurationsparameter für das E-Mail-Benachrichtigungssystem

Über die folgenden Konfigurationsparameter kann das E-Mail-Benachrichtigungssystem konfiguriert werden.

Tabelle 53: Allgemeine Konfigurationsparameter für die Mailbenachrichtigung

Konfigurationsparameter	Bedeutung
Common | InternationalEMail	Gibt an, ob internationale Domänennamen beziehungsweise Unicode-Zeichen in E-Mail-Adressen unterstützt werden. WICHTIG: Der Mailserver muss diese Funktion ebenfalls unterstützen. Gegebenenfalls müssen Sie das Skript `VID_IsSMTPAddress` überschreiben.
Common | MailNotification	Gibt an, ob die weiteren Konfigurationsparameter mit Angaben zu Benachrichtigungen wirksam werden.
Common | MailNotification | AcceptSelfSignedCert	Gibt an, ob selbstsignierte Zertifikate für TLS-Verbindungen akzeptiert werden.
Common | MailNotification | AllowServerNameMismatchInCert	Gibt an, ob nicht passende Servernamen bei den Zertifikaten für TLS-Verbindungen zulässig sind.
Common | MailNotification | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen.
Common | MailNotification | DefaultCulture	Standardsprachkultur, in der E-Mail-Benachrichtigungen versendet werden, wenn für einen Empfänger keine Sprachkultur ermittelt werden kann. Zulässig sind alle Sprachkulturen aus der Tabelle `QBMCulture`.
Common | MailNotification | DefaultLanguage	Standardsprache, in der E-Mail-Benachrichtigungen versendet werden. Zulässig sind alle aktiven Sprachen aus der Tabelle `DialogLanguage`.

Konfigurationsparameter	Bedeutung

Common | MailNotification | DefaultSender	Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.
	Syntax:
	`sender@example.com`
	Beispiel:
	`NoReply@company.com`
	Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.
	Beispiel:
	`One Identity <NoReply@company.com>`

Common | MailNotification | Encrypt	Gibt an, ob E-Mails verschlüsselte werden sollen.
Common | MailNotification | Encrypt | ConnectDC	Domänen-Controller der abzufragenden Domäne, der verwendet werden soll.
Common | MailNotification | Encrypt | ConnectPassword	Kennwort des Benutzerkontos. Die Angabe ist optional.
Common | MailNotification | Encrypt | ConnectUser	Benutzerkonto, mit dem das Active Directory abgefragt wird. Die Angabe ist optional.
Common | MailNotification | Encrypt | DomainDN	Definierter Name der abzufragenden Domäne.
Common | MailNotification | Encrypt | EncryptionCertificateScript	Der Konfigurationsparameter enthält das Skript, welches eine Liste von Verschlüsselungszertifikaten liefert (Standard: `QBM_GetCertificates`).
Common | MailNotification | NotifyAboutWaitingJobs	Gibt an, ob eine Benachrichtigung gesendet werden soll, wenn Prozessschritte eines bestimmten Ausführungszustandes in der Jobqueue sind.
Common | MailNotification | SignCertificateThumbprint	SHA1-Fingerabdruck des zur Signierung zu verwendenden Zertifikats. Dieses kann im Zertifikatsspeicher des Computers oder des Benutzers liegen. HINWEIS: Stellen Sie sicher, dass der private Schlüssel im Zertifikat als exportierbar markiert ist.

Konfigurationsparameter	Bedeutung
Common | MailNotification | SMTPAccount	Name des Benutzerkontos zur Authentifizierung am SMTP Server.
Common | MailNotification | SMTPDomain	Domäne des Benutzerkontos zur Authentifizierung am SMTP Server.
Common | MailNotification | SMTPPassword	Kennwort des Benutzerkontos zur Authentifizierung am SMTP Server.
Common | MailNotification | SMTPPort	Port des SMTP-Dienstes auf dem SMTP Server. Standard: **25**
Common | MailNotification | SMTPRelay	SMTP-Server, der zum Versenden von E-Mail-Benachrichtigungen genutzt wird. Ist kein Server angegeben, wird **localhost** verwendet.
Common | MailNotification | SMTPUseDefaultCredentials	Gibt an, welche Anmeldeinformationen für die Authentifizierung am SMTP Server verwendet werden. Ist der Konfigurationsparameter aktiviert, werden zur Authentifizierung am SMTP Server die Anmeldeinformationen des One Identity Manager Service verwendet. Ist der Konfigurationsparameter nicht aktiviert, werden die in den Konfigurationsparametern **Common | MailNotification | SMTPDomain** und **Common | MailNotification | SMTPAccount** oder **Common | MailNotification | SMTPPassword** hinterlegten Anmeldeinformationen verwendet. (Standard)
Common | MailNotification | TransportSecurity	Verschlüsselungsverfahren beim Versenden von E-Mail-Benachrichtigungen. Wenn keine der folgenden Optionen angegeben wird, richtet sich das Verhalten nach dem Port (Port 25: ohne Verschlüsselung; Port 465: mit SSL/TLS Verschlüsselung). Zulässige Werte sind: • **Auto**: Automatische Erkennung des Verschlüsselungsverfahrens. • **SSL**: Verschlüsseln der gesamten Sitzung mit SSL/TLS. • **STARTTLS**: Verwenden der STARTTLS-Mailserver-Erweiterung. Schaltet die TLS-Verschlüsselung nach dem Greeting und dem

Konfigurationsparameter	Bedeutung
	Lesen der Capabilities des Servers an. Die Verbindung scheitert, wenn der Server die STARTTLS-Erweiterung nicht unterstützt. • **STARTTLSWhenAvailable**: Verwenden der STARTTLS-Mailserver-Erweiterung, wenn verfügbar. Schaltet die TLS-Verschlüsselung nach dem Greeting und dem Lesen der Capabilities des Servers an, jedoch nur, wenn dieser die STARTTLS-Erweiterung unterstützt. • **None**: Keine Sicherheit der Transportschicht. Alle Daten werden als Klartext gesendet.
Common | MailNotification | VendorNotification	E-Mail Adresse der Kontaktperson ihres Unternehmens. Die E-Mail-Adresse wird als Antwortadresse für die Lieferantenbenachrichtigung verwendet. Ist der Konfigurationsparameter aktiviert, erzeugt der One Identity Manager einmal im Monat eine Liste der Systemeinstellungen und sendet die Liste an One Identity. Diese Liste enthält keine personenbezogenen Daten. Sie können die aktuellsten Systeminformationen jederzeit aus dem Menü **Hilfe > Info** überprüfen. Die Liste wird von unserem Kunden-Support-Team proaktiv überprüft, welches nach wesentlichen Änderungen schaut um mögliche Probleme zu identifizieren bevor sie sich auf Ihrem System verwirklichen. Die Listen können von unseren F&E-Mitarbeitern für die Analyse, Diagnose und Replikation zu Testzwecken verwendet werden. Diese Informationen behalten Gültigkeit, solange Ihr Unternehmen weiterhin Pflegeleistungen für dieses Produkt bezieht.

Tabelle 54: Zusätzliche Konfigurationsparameter für E-Mail-Adressen für die Mailbenachrichtigung

Konfigurationsparameter	Beschreibung
QER | Attestation | DefaultSenderAddress	Standard E-Mail-Adresse des Absenders zum Versenden von automatisch generierte Benachrichtigungen über Attestierungsvorgänge. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.
QER | ComplianceCheck |	Standard E-Mail-Adresse des Absenders zum Versenden

Konfigurationsparameter	Beschreibung
EmailNotification | DefaultSenderAddress	von automatisch generierten Benachrichtigungen über Regelprüfungen. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.
QER | ITShop | DefaultSenderAddress	Standard E-Mail-Adresse des Absenders zum Versenden von automatisch generierte Benachrichtigungen über Bestellungen. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.
QER | Policy | EmailNotification | DefaultSenderAddress	Standard E-Mail-Adresse des Absenders zum Versenden von automatisch generierten Benachrichtigungen bei der Überprüfung von Unternehmensrichtlinien. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.
QER | RPS | DefaultSenderAddress	Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen über Berichtsabonnements. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.
TargetSystem | ADS | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem Active Directory.
TargetSystem | ADS | Exchange2000 | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem Microsoft Exchange.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Standard-E-Mail-Adresse zum Versenden von Warnmails.
TargetSystem | AzureAD | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem Azure Active Directory.
TargetSystem | AzureAD | ExchangeOnline | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem Exchange Online.
TargetSystem | CSM | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Cloud -Zielsystem.
TargetSystem | EBS | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem Oracle E-Business Suite.
TargetSystem | LDAP | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem LDAP.
TargetSystem | NDO | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem HCL Domino.

Konfigurationsparameter	Beschreibung
TargetSystem | SAPR3 | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem SAP R/3.
TargetSystem | SharePoint | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem SharePoint.
TargetSystem | Unix | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Unix-basierten Zielsystem.
TargetSystem | UNS | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im kundendefinierten Zielsystem.
TargetSystem | PAG | DefaultAddress	Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Privileged Account Management System.

Detaillierte Informationen zum Thema

- Einrichten des E-Mail-Benachrichtigungssystems auf Seite 81

Anhang E

Einsatz der One Identity Manager-Datenbank mit SQL Server AlwaysOn-Verfügbarkeitsgruppen konfigurieren

Nachfolgend werden nur die Einstellungen für die Arbeit mit dem One Identity Manager beschrieben. Ausführliche Informationen über SQL Server AlwaysOn-Verfügbarkeitsgruppen finden Sie unter Always On availability groups: a high-availability and disaster-recovery solution.

HINWEIS: Wenn eine One Identity Manager-Datenbank in eine SQL Server AlwaysOn-Verfügbarkeitsgruppe aufgenommen werden soll, beachten Sie, dass eine Verfügbarkeitsgruppe pro Verfügbarkeitsdatenbank erforderlich ist.

Beispiel:

Zwei Datenbanken (beispielsweise UAC und QA) sollen als Verfügbarkeitsdatenbanken Teil einer SQL Server AlwaysOn-Verfügbarkeitsgruppe sein. Für jede Datenbank ist eine eigene Verfügbarkeitsgruppe (beispielsweise AGUAC und AGQA) erforderlich.

Voraussetzung

Es wurde ein Failover Cluster Manager konfiguriert. Führen Sie daher den Server Manager auf dem Datenbankserver aus und installieren Sie die Funktion **Failover Clustering**.

Installieren des One Identity Manager

1. Führen Sie das Programm Configuration Wizard gegen einen Clusterknoten aus und folgen Sie den Installationsanweisungen.
2. Installieren und starten Sie den One Identity Manager Service. Nachdem alle Prozesse in der Jobqueue abgearbeitet wurden, stoppen Sie den One Identity Manager Service.
3. Führen Sie den Designer aus und richten Sie die Staging-Ebene für die Datenbank ein.

4. Ändern Sie im SQL Server Management Studio das Wiederherstellungsmodell für die One Identity Manager-Datenbank von **Einfach** auf **Vollständig**.
5. Erstellen Sie eine vollständige Sicherung der Datenbank.
6. Vergewissern Sie sich, dass die Firewall so konfiguriert ist, dass sie die Clusterkommunikation unterstützt.
7. Führen Sie den SQL Server Configuration Manager aus und suchen Sie den SQL Server-Dienst. Öffnen Sie die Eigenschaften und aktivieren Sie **Always-On-Verfügbarkeitsgruppen**. Starten Sie den SQL Server-Dienst auf allen Knoten neu.

   Ausführliche Informationen finden Sie unter Enable or Disable Always On availability group feature.

Konfigurieren der SQL Server AlwaysOn-Verfügbarkeitsgruppen

1. Verbinden Sie im SQL Server Management Studio die Serverinstanz, die den primären Knoten hostet. Um die Verfügbarkeitsgruppen zu konfigurieren, navigieren Sie zu **AlwaysOn High Availability**, klicken Sie auf die rechte Maustaste und wählen Sie **New Availability Group Wizard**.

   Ausführliche Informationen zum Assistenten für neue Verfügbarkeitsgruppen finden Sie im Use the Availability Group Wizard (SQL Server Management Studio).
2. Im Assistenten für neue Verfügbarkeitsgruppen geben Sie den Namen der neuen Verfügbarkeitsgruppe ein und wählen Sie die One Identity Manager-Datenbank aus, die in die neue Verfügbarkeitsgruppe aufgenommen werden soll.
3. Im Assistenten für neue Verfügbarkeitsgruppen erstellen und konfigurieren Sie ein Replikat für die neue Verfügbarkeitsgruppe.
   a. Fügen Sie den sekundären SQL Server-Clusterknoten hinzu.
   b. Aktivieren Sie die automatische Ausfallsicherung und synchrone Übergabe für beide Knoten.
   c. Machen Sie alle Knoten zu einem lesbaren Sekundärknoten; wählen Sie den Wert **Yes**.
   d. Geben Sie einen Verfügbarkeitsgruppen-Listener an.

      Verwenden Sie beispielsweise für den DNS-Namen denselben Namen wie die Verfügbarkeitsgruppe, jedoch mit dem Suffix "L", und verwenden Sie Port 1433. Weisen Sie eine IP-Adresse im gleichen Subnetz wie der SQL Server zu.

      Ausführliche Informationen finden Sie unter Specify Replicas Page (New Availability Group Wizard: Add Replica Wizard).
4. Im Assistenten für neue Verfügbarkeitsgruppen legen Sie die Einstellungen für die Datensynchronisation fest. Die Einstellungen für die Datensynchronisierung hängen von Ihrer Infrastruktur ab.

   Wenn Sie eine Netzwerkfreigabe für die Datensynchronisierung zwischen den Replikaten verwenden, wählen Sie die Option **Full** und geben Sie den Netzwerkstandort an. Serverinstanzen, die ein Replikat hosten, benötigen Lese- und Schreibzugriff auf die Freigabe.

Konfigurieren des One Identity Manager

1. Führen Sie das Programm Database Compiler aus. Verbinden Sie sich mit dem primären Knoten und kompilieren Sie die Datenbank. Ändern Sie zu diesem Zeitpunkt nicht die Verbindungsdaten der Datenbank.

   Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
2. Aktualisieren Sie anschließend die Datenbankverbindungsdaten im Designer.
   a. Starten Sie den Designer und verbinden Sie sich mit dem primären Knoten.
   b. Wählen Sie im Designer die Kategorie **Basisdaten > Allgemein > Datenbanken**.
   c. Wählen Sie im Listeneditor die Datenbank.
   d. Wählen Sie die Aufgabe **Verbindungsparameter für Datenbank definieren**.
   e. Geben Sie die Verbindungsdaten zur Datenbank an. Verwenden Sie den DNS-Namen des Listeners anstelle des Servernamens.

   Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
3. Führen Sie das Programm Database Compiler aus und kompilieren Sie die Datenbank. Verwenden Sie den Listener.
4. Führen Sie das Job Service Configuration aus und ändern Sie die Verbindungsdaten für den One Identity Manager Service. Verwenden Sie den Listener.

   Es wird empfohlen, die Queue-Bezeichnung zu ändern, um den Cluster besser widerzuspiegeln. Beachten Sie, dass Sie den Namen der Queue auch im Designer aktualisieren.

   Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
5. Stellen Sie sicher, dass Jobserver, Anwendungsserver, Frontends, Webanwendungen und Synchronisierungsprojekte den Listener verwenden, um sich bei der Datenbank anzumelden.

Verwandte Themen

- Installieren und Konfigurieren einer One Identity Manager-Datenbank auf Seite 58
- Installieren und Konfigurieren des One Identity Manager Service auf Seite 89
- Anmelden an den One Identity Manager-Werkzeugen auf Seite 178
- Datenbankfehler bei der Migration einer Datenbank in SQL Server AlwaysOn-Verfügbarkeitsgruppen auf Seite 193

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

E

F

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W