

One Identity Manager 8.1

Versionshinweise

März 2019

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 8.1 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 8.0.2 aufgeführt.

One Identity Manager 8.1 ist ein Minor Release mit neuen Funktionen und verbessertem Verhalten. Siehe [Neue Funktionen](#) auf Seite 3 und [Verbesserungen](#) auf Seite 9.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.0.2 ist, lesen Sie auch die Versionshinweise der vorangegangenen Versionen. Die Versionshinweise finden Sie unter [One Identity Manager Support](#).

Informationen über Änderungen in der Data Governance Edition finden Sie in den *One Identity Manager Data Governance Edition Release Notes*.

Informationen über Änderungen im ServiceNow Modul finden Sie in den *One Identity Manager and ServiceNow Integration Release Notes*.

Informationen über Änderungen im Cloud HR Systems Modul finden Sie in den *One Identity Manager and Cloud HR Systems Integration Release Notes*.

Die One Identity Manager Dokumentation liegt sowohl in englischer als auch deutscher Sprache vor. Für die nachfolgend aufgeführten Dokumente gibt es nur eine englische Fassung:

- One Identity Manager Password Capture Agent Administration Guide
- One Identity Manager LDAP Connector for CA Top Secret Reference Guide
- One Identity Manager LDAP Connector for IBM RACF Reference Guide
- One Identity Manager LDAP Connector for IBM AS/400 Reference Guide
- One Identity Manager LDAP Connector for CA ACF2 Reference Guide
- One Identity Manager REST API Reference Guide
- One Identity Manager Web Runtime Documentation
- One Identity Manager Object Layer Documentation

- One Identity Manager Composition API Object Model Documentation
- One Identity Manager Secure Password Extension Administration Guide

Über One Identity Manager 8.1

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,
- 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 Hybrid Subscription

Die neueste Version unserer On-Prem-Produkte bietet eine obligatorische One Identity Hybrid Subscription, die unseren Kunden den Übergang zu einer hybriden Umgebung auf ihrem Weg in die Cloud erleichtert. Die Subscription ermöglicht es Ihnen, ihre On-Prem-Lösungen mit unserer One Identity Starling software-as-a-service-Plattform zu verbinden. Geben Sie Ihrem Unternehmen umgehenden Zugriff auf eine Reihe von Funktionen und Services, die von der Cloud bereitgestellt werden und die Möglichkeiten Ihres On-Prem-Produkts erweitern. Wir werden kontinuierlich neue Produkte und Funktionen für unsere One Identity SaaS-Plattform zur Verfügung stellen. Mit der One Identity Hybrid Subscription können Sie diese sofort für Ihre One Identity On-Prem-Lösungen nutzen, und ihre Subscription bringt weiterhin einen Mehrwert.

Erweitern Sie den Funktionsumfang von One Identity Manager mit einer [One Identity Hybrid Subscription](#), welche eine Vielzahl zusätzlicher Cloud-Funktionen und -Services bietet. Verwenden Sie die universelle [Starling Two-Factor Authentication](#) um den administrativen Zugriff zu schützen, um eine zusätzliche Authentifizierung zu erzwingen, wenn Sie einen kritischen Zugriff anfordern oder genehmigen oder um die Out-of-Band Benutzerverifizierung für Kennwortanforderungen zu aktivieren. Gegen Aufpreis können diese Angebote auch auf weitere Zielsysteme und Anwendungsfälle ausgeweitet werden. Eine einzige Subscription kann für alle Ihre One Identity-Produkte verwendet werden.

Neue Funktionen

Neue Funktionen in One Identity Manager 8.1.

Basisfunktionen

- Die minimalen Systemvoraussetzungen finden Sie unter [Systemanforderungen](#) auf Seite 66.
- Oracle Database als Datenbanksystem für die One Identity Manager-Datenbank wird nicht mehr unterstützt.
- One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe. Der Datenbankserver muss die extreme Transaktionsverarbeitung (XTP) unterstützen. Beachten Sie dazu die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 74.
- Unterstützung von abgestuften Berechtigungen auf Serverebene und Datenbankebene.

Es werden SQL Server Anmeldungen und Datenbankbenutzer mit den erforderlichen Berechtigungen für den administrative Benutzer, Konfigurationsbenutzer und Endbenutzer bereitgestellt. Beachten Sie dazu die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 74. Ausführliche Informationen zu den Berechtigungen finden Sie im *One Identity Manager Installationshandbuch*.

Einige Frontends erwarten mindestens die Berechtigungen eines Konfigurationsbenutzers. Die Anmeldung als Endbenutzer wird in diesem Fall nicht unterstützt. Im Anmeldedialog wird zusätzlich die Berechtigungsebene für den verwendeten Benutzer dargestellt.

- Die Frontends prüfen vor dem Start, ob der Benutzer die benötigten Berechtigungen hat. Das Starten der Frontends ist nur zulässig, wenn der Benutzer die entsprechenden Programmfunktionen über seine Rechtegruppen besitzt. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
- Rollenbasierte Rechtegruppe können an eine Anwendung zugewiesen werden. Die Berechtigungen der Rechtegruppe gelten nur für diese Anwendung. Meldet sich ein Benutzer an der Anwendung an, erhält er die Berechtigungen der Rechtegruppe zusätzlich zu seinen anderen Berechtigungen.
- Abmeldungen vom One Identity Manager können im Systemprotokoll aufgezeichnet werden. Zur Aufzeichnung aktivieren Sie den Konfigurationsparameter **Common | Journal | LogoffAudit**. Anmeldungen und Abmeldungen können über die View `QBM_VDialogJournalLoginAudit` ausgewertet werden.
- Verbesserte Unterstützung bei der Fehlerbehebung.
 - Der Object Browser unterstützt das Debuggen von Skripten, Bildungsregeln, Formatskripten, Tabellenskripten, Prozessen und Methoden.

Um lokale Debug-Assemblies zu erzeugen, aktivieren Sie im Database Compiler die Option **Debuginformationen erzeugen** und wählen Sie die Kompilervorgabe **Skripte inkl. aller Abhängigkeiten**. Die Option ist nur für Benutzer verfügbar, die die Programmfunktion **Erlaubt das Erstellen lokaler Debug-Assemblies** (Common CompileForDebug) über ihre Rechtegruppe erhalten. Die Programmfunktion muss einer kundenspezifischen Rechtegruppe zugewiesen sein.

- Im System Debugger können Skripte gesucht werden. Geänderte Skripte werden mit einem * gekennzeichnet. Es können mehrere Skripte gleichzeitig gespeichert werden.
- Um den System Debugger oder die Debug-Funktion im Object Browser zu nutzen, muss Visual Studio Version 2017 mit dem aktuellem Service Pack sowie Microsoft .NET Framework Version 4.7.2 Developer Pack oder höher installiert sein.
- Im Fehlermeldungsfenster der Frontends kann die Windows Schrittaufzeichnung gestartet werden, um die Schritte zum Fehler aufzuzeichnen.
- Unterstützung von NLog 4.5.11.
- Anzeige des Protokolls im Anwendungsserver. Das Protokoll ist nur für Benutzer sichtbar, die die Programmfunktion **Aktiviert die Protokollanzeige im Anwendungsserver** (AppServer_Logs) über ihre Rechtegruppe erhalten.
- Für die Installation eines Anwendungsservers wird ein Kommandozeilenprogramm AppServer.Installer.CMD.exe bereitgestellt. Das Programm finden Sie im Add-On für das Konfigurationsmodul.
- Verbesserte OAuth 2.0/OpenID Connect Konfiguration.

Für die Erstellung der OAuth 2.0/OpenID Connect Konfiguration im One Identity Manager wird im Designer ein Assistent angeboten. Die Konfigurationsdaten können über OpenID Connect Discovery ermittelt werden oder manuell erfasst werden. Die Abbildung der Informationen im One Identity Manager Schema erfolgt in eigenen Tabellen.

HINWEIS: Bei der Aktualisierung einer One Identity Manager-Datenbank werden vorhandene Werte aus Konfigurationsparametern und den Einstellungen für Webserver in die neuen Datenstruktur übernommen.

Der Konfigurationsparameter **QER | Person | OAuthAuthenticator** und seine untergeordneten Konfigurationsparameter wurden gelöscht.

Prüfen Sie im Designer unter **Basisdaten | Sicherheitseinstellungen** die OAuth 2.0/OpenID Connect Konfiguration sowie die Einstellungen der Webserver.

- Erweiterte Unterstützung von JSON Web Key für die OAuth 2.0/OpenID Connect Authentifizierung.
- Für den Import von Schemaerweiterungen wird ein Kommandozeilenprogramm SchemaExtensionCmd.exe bereitgestellt. Das Programm benötigt eine Definitionsdatei

(XML-Datei), die im Programm Schema Extension erzeugt werden kann. In der Definitionsdatei können mehrere Erweiterungen angegeben werden.

Kundenspezifische Schemaerweiterungen auf Datenbanken mit einer Staging-Ebene **Testumgebung** oder **Entwicklungssystem** können mit dem Programm Schema Extension und mit dem Kommandozeilenprogramm wieder entfernt werden.

- Verbesserte Unterstützung der Kennwortprüfung.
 - Es können mehrere Kennwortfragen und Kennwortantworten festgelegt werden. Wie viele Kennwortfragen festgelegt werden und zu beantworten sind, wird über die Konfigurationsparameter **QER | Person | PasswordResetAuthenticator | QueryAnswerDefinitions** und **QER | Person | PasswordResetAuthenticator | QueryAnswerRequests** gesteuert. Der Konfigurationsparameter **QER | Person | PasswordResetAuthenticator | InvalidateUsedQuery** definiert, ob Fragen nach erfolgreicher Kennworrücksetzung nicht mehr verwendet werden dürfen.
 - Kennwortrichtlinien können an Abteilungen, Kostenstellen, Standorte und Geschäftsrollen zugewiesen werden.
 - Kennwortrichtlinien können abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten angewendet werden.
 - Für Kennwortrichtlinien können Zeichenklassen festgelegt werden, die in generierten Kennwörtern nicht enthalten sein dürfen.
 - Ob eine Spalte Namensbestandteile für die Prüfung in Kennwortrichtlinien enthält, kann über die Spaltendefinitionen festgelegt werden.
 - Das zentrale Kennwort einer Person wird auf das Systembenutzerkennwort der Person abgebildet. Das Verhalten wird über den Konfigurationsparameter **QER | Person | UseCentralPassword | SyncToSystemPassword** definiert.
 - ❗ **HINWEIS:** Der Konfigurationsparameter **QER | Person | UseCentralPassword | PasswordCaptureAgent | SyncSystemPassword** wurde entfernt. Das Skript `VI_CaptureAgent_SetPassword` wurde angepasst. Wenn Sie das Skript kundenspezifisch überschrieben haben, übernehmen Sie die Änderungen.
 - Das zentrale Kennwort einer Person wird in der Historie der Benutzerkontenkennwörter vermerkt und bei der Kennwortprüfung berücksichtigt.
 - ❗ **HINWEIS:** Wenn Sie kundenspezifische Bildungsregeln für Kennwortspalten definiert haben, prüfen Sie, ob diese in das Skript `QER_Publish_CentralPassword` verlagert werden sollte. Überschreiben Sie dazu das Skript.
 - Bei Eingabe des zentralen Kennwortes einer Person werden gesperrte Systembenutzeranmeldungen, Active Directory Benutzerkonten und SAP Benutzer entsperrt. Das Verhalten wird über die Konfigurationsparameter **QER**

| Person | UseCentralPassword | SyncToSystemPassword | UnlockByCentralPassword, TargetSystem | ADS | Accounts | UnlockByCentralPassword und **TargetSystem | SAPR3 | Accounts | UnlockByCentralPassword** gesteuert.

- Vier-Augen-Prinzip für Vergabe des Zugangscodes. Über den Konfigurationsparameter **QER | Person | PasswordResetAuthenticator | PasscodeSplit** wird gesteuert, ob ein durch den Helpdesk generierter Zugangscodes in zwei Bestandteile aufgeteilt wird, einen für den Helpdesk und einen für den Manager der Person.
- Bei der personenbasierten Anmeldung werden kundenspezifische Kennwortrichtlinien beachtet.
- Um mehr Sicherheit zu gewährleisten, wird das Captcha zusammen mit dem Zugangscodes, den Kennwortfragen und dem Kennwort abgefragt.
- Zusätzliche Spracheinstellungen für die Formatierung von Daten wie beispielsweise Datumsformate, Zeitformate oder Zahlenformate für Benutzer.
 - In den Programmeinstellungen der Frontends können die Sprache für die Anzeigetexte und die Sprache für die Darstellung von Werten getrennt festgelegt werden.
 - In den Personenstammdaten kann eine Sprache zur Wertermittlung hinterlegt werden.
 - Über den Konfigurationsparameter **Common | MailNotification | DefaultCultureFormat** kann die Standardsprache für die sprachspezifische Formatierung von Werten für Personen festgelegt werden.
- Die Verschlüsselung der Datenbank verwendet RSA-Verschlüsselung mit Optimal Asymmetric Encryption Padding (OAEP). Bereits verschlüsselte Datenbanken mit einer Schlüssellänge > 1024 Bit werden nicht konvertiert, sondern nutzen weiterhin PKCS#1 für die Verschlüsselung. Neu verschlüsselte Werte nutzen OAEP. Wenn Sie noch einen Schlüssel mit einer Länge 1024 Bit einsetzen, wird empfohlen, dass Sie einen neuen Schlüssel im Crypto Configuration erstellen und die Datenbank neu verschlüsseln.
- Im Installationsassistenten können die Einstellungen für die Installation eines Dienstes geändert werden, wenn diese von der Standardinstallation abweichen sollen.
- Für die Kompilierung der Datenbank und die Kompilierung der Skripte für Synchronisationsprojekte wird die .NET Compiler Plattform verwendet.
- In den Spaltendefinitionen können Skripte zum bedingten Entfernen der Sichtbarkeitsrechte und Bearbeitungsrechte der Spalten definiert werden.

Webanwendungen

- Mit dem API Designer können Sie auf schnellstem Wege eine REST API erstellen, dokumentieren, kompilieren und veröffentlichen. Diese API basiert auf der OpenAPI-Spezifikation und dem One Identity Manager-Datenbankmodell. Die Vorteile des API

Designers auf einen Blick:

- Einfache und schnelle Bedienung.
- Die fertige API versteht das One Identity Manager-Datenbankmodell.
- Änderungen an der API sind nachvollziehbar.
- Unterstützt die Prinzipien eines guten API-Designs.
- APIs, die Sie mithilfe des API Designers erstellen, basieren grundsätzlich auf der OpenAPI-Spezifikation.

Ausführliche Informationen finden Sie im *One Identity Manager API Designer Benutzer- und Entwicklungshandbuch* und im *One Identity Manager HTML5-Entwicklungshandbuch*.

- Der API Server stellt die API zur Verfügung, die Sie mithilfe des neuen API Designers erstellen.
- Das Web Portal für Betriebsunterstützung wurde grundlegend als HTML5-Anwendung neu erstellt. Die zugrundeliegende REST API wurde mithilfe des neuen API Designers erstellt.
- Implementierung von Secure Password Extension, um Benutzern den Zugriff auf das Kennworrücksetzungsportal über den Windows-Anmeldebildschirm zu ermöglichen. Secure Password Extension ist eine Anwendung, die mit einem Klick über den Windows-Anmeldebildschirm auf die gesamte Funktionalität des Kennworrücksetzungsportal zugreifen kann.

Secure Password Extension ist ein Add-on für das Active Directory Modul. Ausführliche Informationen zur Konfiguration und Verteilung der Secure Password Extension finden Sie im *One Identity Manager Secure Password Extension Administration Guide*.

- Benutzer, die sich selbst für das Web Portal registrieren, erhalten eine Bestätigungse-Mail mit einem Link auf eine Bestätigungsseite. Auf dieser Seite kann der Benutzer seine Registrierung selbstständig abschließen und anschließend das Kennwort zur Anmeldung an den One Identity Manager-Werkzeugen initial setzen.

Neue Konfigurationsparameter: **QER | Attestation | ApproveNewExternalUsers, QER | Attestation | NewExternalUserTimeoutInHours, QER | Attestation | NewExternalUserFinalTimeoutInHours, QER | Attestation | MailTemplateIdents | NewExternalUserVerification** und **QER | WebPortal | PasswordResetURL**

Neue Anwendungsrolle: **Basisrollen | Selbstregistrierte Personen**

- Verschiedene Statusmeldungen können nun als Browser-Benachrichtigung angezeigt werden.

Neue Web Designer Konfigurationsparameter: **VI_Common_EnableNotifications** und **VI_Common_NotificationPollingInterval**

Zielsystemanbindung

- Neues Privileged Account Governance Modul zur Verwaltung von Privileged Account Management Systemen im One Identity Manager.

Im One Identity Manager können Benutzerkonten erstellt und bearbeitet werden. Über Benutzergruppen erhalten Benutzerkonten die erforderlichen Nutzungsrechte, um den Zugriff auf privilegierte Systeme im Privileged Account Management System anfordern zu können. Benutzerkonten, Benutzergruppen und Zugriffsanforderungen auf privilegierte Systeme können im Web Portal bestellt werden.

Mit dem One Identity Safeguard Konnektor können Benutzerkonten, Benutzergruppen, Assets, Assetgruppen, Assetkonten, Verzeichnisse, Verzeichniskonten, Kontogruppen, Nutzungsrechte und Zugriffsanforderungsrichtlinien einer One Identity Safeguard Appliance in den One Identity Manager eingelesen werden. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzerkonten und Systemberechtigungen, IT Shop oder Berichtsabonnements für Privileged Account Management Systeme zu nutzen.

Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Privileged Account Governance*.

- Im Windows Systemmonitor können Leistungsdaten zur Zielsystemsynchronisation angezeigt werden. Die Performanceüberwachung kann in der Konfigurationsdatei des Synchronization Editor (`SynchronizationEditor.exe.config`) aktiviert werden. Damit die One Identity Manager Leistungsindikatoren ausgewählt werden können, muss der Synchronization Editor als Administrator gestartet werden.
- Änderungen an einem einzelnen Objekt im Zielsystem können sofort in die One Identity Manager-Datenbank übertragen werden, ohne dass eine vollständige Synchronisation der Zielsystem-Umgebung gestartet werden muss. Diese Einzelobjektsynchronisation kann im Manager für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert. Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.
- Es können synchronisationsprojektübergreifende Startfolgen für die vollständige Synchronisation definiert werden. Damit können die Startkonfigurationen für verschiedene Zielsysteme in eine Reihenfolge gebracht werden. Die Synchronisationen werden nacheinander ausgeführt. Über den Konfigurationsparameter **DPR | StartSequence | LifeTime** wird der Aufbewahrungszeitraum für abgeschlossene Startfolgen festgelegt.
- Der native Datenbankkonnektor ermöglicht es, das Konnektorschema mit virtuellen Schemaeigenschaften zu erweitern. Für die betreffende Tabelle muss eine Datenoperation definiert werden, welche die virtuelle Schemaeigenschaft nutzt. Diese Schemaeigenschaft kann anschließend genau definiert werden.
- Der Synchronization Editor stellt eine Skriptbibliothek bereit. Alle hier definierten Skripte können in anderen Skripten des Synchronisationsprojekts genutzt werden. Skripte, die als Skriptvorlage gekennzeichnet wurden, können in beliebige andere

Synchronisationsprojekte importiert, dort angepasst und weiter genutzt werden. Die Skripte von Skripteigenschaften können in die Skriptbibliothek verschoben werden.

- Vor dem Löschen eines G Suite Benutzerkontos können die Nutzerdaten an ein anderes Benutzerkonto übertragen werden. Das Benutzerkonto wird erst dann im Zielsystem gelöscht, wenn der Datentransfer erfolgreich abgeschlossen ist. Dieses Verhalten kann an den Zielsystemverbindungen konfiguriert werden. Diese Funktion kann nur in neu erstellten Synchronisationsprojekten genutzt werden.
- Die Zugriffsberechtigungen für die SAP Tochtersisteme einer Zentralen Benutzerverwaltung können sowohl über Direktzuweisung als auch über IT Shop-Bestellungen und indirekte Zuweisung gewährt werden. Dafür werden Kontendefinitionen eingesetzt.

HINWEIS: Bis Version 8.0 wurde der Zugriff auf das Zentralsystem automatisch gegeben (Eintrag in der Tabelle SAPUserInSAPMandant). Ab Version 8.1 muss dieser Zugriff explizit gewährt werden (Eintrag in der Tabelle SAPUserMandant). Bereits vorhandene Zuweisungen aus SAPUserInSAPMandant werden bei der Migration der One Identity Manager-Datenbank in Direktzuweisungen umgewandelt. Die Zugriffsberechtigungen auf das Zentralsystem bleiben damit erhalten.

Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#28147 und VPR#28147_2 bereitgestellt.

- SAP Parameter können über Geschäftsrollen und Organisation an SAP Benutzerkonten vererbt werden.

Identity Management und Access Governance

- Die Verantwortlichen von Systemrollen, Applikationen und abonnierbaren Berichten können Bestellungen dieser Objekte im Web Portal bearbeiten. Dafür werden die Verantwortlichen automatisch in die neuen Anwendungsrollen für die Produkteigner von Systemrollen, Applikationen und abonnierbaren Berichten aufgenommen.
- Neue Konfigurationsparameter unter **QER | Person| Starling** zur Unterstützung der One Identity Hybrid Subscription.

Siehe auch:

- [Verbesserungen](#) auf Seite 9
- [Gelöste Probleme](#) auf Seite 30
- [Schemaänderungen](#) auf Seite 49
- [Patches für Synchronisationsprojekte](#) auf Seite 58


Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die im One Identity Manager 8.1 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Für Prozessfunktionen und Prozesse kann definiert werden, ob bei der Prozessverarbeitung auf die Verarbeitung von DBQueue Prozessor Aufträgen gewartet werden soll.	28087
Verbesserungen bei der Generierung von Berichten. <ul style="list-style-type: none">Die Generierung von Berichten in den Frontends kann über die Schaltfläche Abbruch abgebrochen werden.Die Prozesskomponente ReportComponent besitzt einen neuen Parameter LimitRows, um die maximale Anzahl der pro Abfrage zurückgegebenen Zeilen, festzulegen.	28921, 17407, 15696
Verbesserter Export von Berichten. <ul style="list-style-type: none">Die Prozessfunktion Export der Prozesskomponente ReportComponent besitzt neue Parameter für den Export von Berichten als Microsoft Excel-Dateien.An der Prozessfunktion SendRichMail der Prozesskomponente MailComponent stehen jetzt Parameter zur Verfügung, um Berichte in verschiedenen Formaten als Anhang zu versenden.	19107
Verbesserungen für Berichte mit Abfragen historischer Daten. <ul style="list-style-type: none">Mit dem Abfragemodul Historische Zuordnungen können Abfragen auf Fremdschlüsselobjekte erstellt werden.Für die Abfragemodule Historie eines Einzelobjektes und Historie mehrerer Objekte können die Spalten festgelegt werden, für welche die Änderungen im Bericht dargestellt werden sollen.Für die Abfragemodule Historie mehrerer Objekte und Historische Zuordnungen können mehrere Kriterien definiert werden.Die Datenabfrage für das Abfragemodul Historische Zuordnungen liefert zusätzlich die Spalten origin und originDisplay zur Abfrage von Zuweisungsarten.	21158, 21159, 22003, 29816
Verbesserung der Zuweisung von Methodendefinitionen (DialogMethod) zu Objektdefinitionen (DialogObject).	30462, 30514
Detaillierter Lizenzbericht im License Meter.	30321
Verbesserte Unterstützung des Transports. <ul style="list-style-type: none">Beim Export im Database Transporter können zu einem Änderungskennzeichen die untergeordneten Änderungskennzeichen gewählt werden.Neuer Dialog zur Lösung von Transportkonflikten.Neuer Transportmodus zum Transportieren von	12732, 28945, 29555

Verbesserung	Fehler ID
Synchronisationsprojekten.	
Die Vorschlagliste der $\$$ -Notation Prozesseditor wurde erweitert. Die Eingabe $\\$PC(\text{VarName})\\$ zeigt in der Vorschlagliste ein Beispiel. Die Eingabe values(zeigt eine Vorschlagliste mit values-Definitionen. Die Eingabe "&out(zeigt eine Vorschlagliste mit Out-Parametern.	16108, 29090
Um auf den Anzeigewert eines alten Wertes einer Spalte zuzugreifen, können die Objekteigenschaften [o] und [d] kombiniert werden.	19641, 17262
Kundenspezifische Konfigurationsparameter können nur noch unter dem Konfigurationsparameter Custom erstellt werden.	30764
<p>i HINWEIS: Bestehende kundenspezifische Konfigurationsparameter werden aus Kompatibilitätsgründen nicht angepasst. Passen Sie diese Konfigurationsparameter bei Bedarf manuell an und prüfen Sie die Verwendung.</p>	
Verbesserte Indizierung des Suchindex.	786112, 30436, 30065
<ul style="list-style-type: none"> Die Indizierung des Suchindex kann über die Konfigurationsparameter Common Indexing BatchSize und Common Indexing Interval konfiguriert werden. Im Fall einer Wiederverwendung des Anwendungspool wird der Suchindex lesend geöffnet. Protokollmeldungen zur Indizierung werden im Protokoll des Anwendungsservers ausgegeben. 	
Verbesserte Protokollierung im Programm Quantum.MigratorCmd.exe.	30412
Über den Konfigurationsparameter QBM DBServerAgent CreateNotification kann festgelegt werden, in welchen Fällen Benachrichtigungen von SQL Server Agent Aufträgen in das Ereignisprotokoll geschrieben werden.	30376
Die Prozessfunktionen der Prozesskomponente HandleObjectComponent wurden um einen optionalen Parameter ProcID zur Übergabe der GenProcID erweitert.	30323
<p>i HINWEIS: Die Standardprozesse wurden angepasst. Kundenspezifische Prozesse passen Sie bei Bedarf manuell an.</p>	
Der Zeitpunkt der letzten Prozessabholung wird für einen Jobserver gespeichert.	30270
Verbesserte Rückmeldung bei der Ausführung von Konsistenzprüfungen.	30193
Beim Erstellen einer neuen Datenbankverbindung bei der Anmeldung wird die Auswahl für Systemtypen nur angezeigt, wenn verschiedene System-	30124

Verbesserung	Fehler ID
typen zulässig sind.	
Verbesserte Navigation und verbesserte Bearbeitung von Objekten im Designer. Verbesserte Anzeige kundenspezifischer Änderungen im Designer.	29864, 29786, 28997, 29001, 29342, 23814
Verbessertes Update-Verhalten für die automatische Softwareaktualisierung.	29886
Die Zuordnung von Authentifizierungsmodulen zu Anwendungen kann deaktiviert werden.	29878
Im Steuerelement zum Setzen eines Datums kann auch die Uhrzeit gesetzt werden.	29870
Formulare mit der Formularvorlage FrmCommonChildRelationGrid zeigen im Tabellenkopf einen Tooltipp zur Spalte.	29022
Im Wörterbucheditor im Designer kann eine Rechtschreibkontrolle ausgeführt werden.	29252
Im Dialog zur Bearbeitung von Änderungskennzeichen können die zugewiesenen Änderungen gefiltert werden.	24098
Spezialisierte Editor für einige Konfigurationsparameter.	29751
Die VI.Base.ViException-Klasse hat jetzt eine Funktion SetSolution zum Setzen des Textschlüssels und der Parameter und einen Parameter Solution zum Abrufen des fertigen Textes für Angabe einer Problemlösung zum Fehler.	29433
Die Prozessfunktionen SendMail und SendRichMail der Prozesskomponente MailComponent wurden um den Parameter TransportSecurity zur Angabe des Verschlüsselungsverfahrens beim Versenden von E-Mail Benachrichtigungen erweitert. Die Parameter EnableSSL, StartTls, StartTlsWhenAvailable und NoTransportSecurity wurden gelöscht.	29662
 HINWEIS: Die Standardprozesse wurden angepasst. Kundenspezifische Prozesse passen Sie bei Bedarf manuell an.	
Verbesserte Unterstützung verzögerter Operationen. <ul style="list-style-type: none"> • Der Menüeintrag Datenbank Verzögerte Operationen anzeigen wird jetzt im Manager immer angezeigt. • Auf Zuordnungsformularen werden verzögerte Operationen für Zuordnungen mit einem eigenen Symbol gekennzeichnet. • Zusätzliche Konfigurationsparameter Common 	21663, 30215, 30734

Verbesserung	Fehler ID
<p>DeferredOperation AllowUpdateInInsertMode und Common DeferredOperation IgnoreMissingOnDelete für die Konfiguration verzögerter Operationen.</p>	
<p>Verbesserte Ausführung von Bildungsregeln über den One Identity Manager Service.</p>	22360, 30730
<p>Unterstützung von dynamisch erzeugtem HTML-Code in Mailvorlagen. In der <code>\$</code>-Notation kann als Typ HTML gewählt werden. HTML-Code in Skripten und Spalten wird dann übernommen und nicht maskiert. Es erfolgt keine Sicherheitsprüfung.</p> <p>Beispielskript mit HTML-Code:</p> <pre>Public Function CCC_HtmlMailText(obj As IEntity) As String Return "<h1 style='color:red'>" & obj.Display & "</h1>" End Function</pre> <p>Aufruf in der Mailvorlage:</p> <pre>\$SCRIPT(CCC_HtmlMailText):HTML\$</pre>	27806
<p>Verbesserungen im Job Queue Info.</p> <ul style="list-style-type: none"> Die Ansicht Betroffene Objekte zeigt alle Objekte, die von einem Prozessschritt betroffen sind. In der Ansicht Verlauf wird die erneute Initialisierung der Jobqueue angezeigt. Zusätzlich erfolgt im Job Queue Info eine Warnmeldung. Mit Klick auf die Meldung werden detaillierte Meldungen ausgegeben. Parameter können mit Mehrfachauswahl kopiert werden. Wenn die DBQueue mehr als 250000 Berechnungsaufträge enthält, wird in der Ansicht DBQueue die Operation There are more tasks to be processed angezeigt. Diese zeigt die Anzahl der Aufträge, die aktuell nicht in der DBQueue-Übersicht angezeigt werden. 	29052, 16641, 28692, 31140
<p>Verbesserungen im Configuration Wizard.</p> <ul style="list-style-type: none"> Verbesserte Überprüfung der SQL Server- und Datenbankeinstellungen im Configuration Wizard bevor die Migration einer One Identity Manager-Datenbank gestartet wird. Bei der Auswahl der Module wird die Modulversion angezeigt. Beim Erstellen einer neuen Datenbank mit dem Configuration Wizard wird bei der Auswahl <Default> zusätzlich der Verzeichnisname angezeigt. Verbesserte Anzeige von Fehlern im Configuration Wizard. 	29224, 29262, 30227, 22575, 31061
<p>Zusätzliche Konsistenzprüfung Differences in usage types in referring tables um Transportprobleme zu verhindern.</p>	29803

Verbesserung	Fehler ID
Verbesserte Auswahl von Werten aus einer Liste mit zulässigen Werten im Where-Klausel-Assistenten.	29024
Die Simulation der Rechte im Designer kann auf ausgewählte Tabellen eingeschränkt werden.	29273
Tabellen vom Typ Read only , Union oder Proxy können nur als sichtbar definiert werden.	29500
Verbesserte Unterstützung von Statistiken. <ul style="list-style-type: none"> • Neuer Editor zum Bearbeiten von Statistikdefinitionen im Designer. • Erweiterung des Steuerelementes für Statistiken. Bei Doppelklick auf die Titelzeile einer Statistik kann ein weiterer Menüeintrag geöffnet werden, beispielsweise um Berichte oder Listen anzuzeigen. Für diese Funktionalität muss unterhalb des Menüeintrags ein weiterer Menüeintrag definiert werden. 	29444, 29145
Die Initialisierung der automatischen Vervollständigung bei der Eingabe von Skript-Code erfolgt jetzt im Hintergrund.	29713
Prozess-ID und Startzeitpunkt externer Prozesse werden in der Webseite des One Identity Manager Service angezeigt.	29718
Verbesserte Unterstützung im Software Loader beim Laden von Dateien für Webanwendungen.	29770
Neue Prozessfunktionen zum Setzen und Entfernen von Zugriffsrechten an der Prozesskomponente FileComponent.	29791
Für datenabhängige Menüeinträge mit einer Liste wird die Anzahl der Listenelemente angezeigt.	30383
Es kann konfiguriert werden, wie lang der Wert von Prozessparametern sein darf, die in der Prozesshistorie aufgezeichnet werden. Neuer Konfigurationsparameter: Common ProcessState JobHistory TrimLongParameters	29606
An Tabellenrelationen kann definiert werden, ob das übergeordnete Objekt in die Liste der von einem Prozess betroffenen Objekte aufgenommen werden soll. Damit kann verhindert werden, dass das übergeordnete Objekt mehrfach gleichzeitig verarbeitet wird.	29421
Optimierung der Objektauswahlskripte für Objekte der Tabelle BaseTree.	22266
Die Überblicksformulare VI_Structure_Locality_Assignments_Overview, VI_Structure_Department_Assignments_Overview, VI_Structure_ProfitCenter_Assignments_Overview und VI_Structure_Org_Assignments_Overview wurden gelöscht.	28988
Der Zeitplaneditor des Designers kann jetzt auch aus dem Launchpad	29045

Verbesserung	Fehler ID
gestartet werden.	
Die Zeitpläne Benutzerkonten ausgeschiedener Personen sperren und Zeitweise deaktivierte Benutzerkonten aktivieren sind jetzt standardmäßig aktiviert.	29045
Personen und Systembenutzer, die aufgrund fehlerhafter Anmeldungen gesperrt sind, werden im Manager und Designer angezeigt. <ul style="list-style-type: none"> • Neue Menüeinträge in der Navigationsstruktur • Tooltip auf den Überblicksformularen 	29095, 29371
Zur besseren Unterstützung von Anwendungsservern wurde die Schnittstelle der Methode <code>Person.OrderShoppingCart</code> geändert. Die Klasse <code>QER.Customizer.ItemInfo</code> enthält jetzt eine <code>ExceptionInfo</code> mit detaillierteren Informationen zum Fehler.	29928
Verbesserungen im Anwendungsserver. <ul style="list-style-type: none"> • Verbesserte Absicherung der API des Anwendungsservers. • Verbesserte Protokollierung im Anwendungsserver. • Verbesserte Gültigkeitsüberprüfung von Verbindungen zum Anwendungsserver. 	30405, 30618, 30315, 31299, 31300
Performanceverbesserungen im DBQueue Prozessor.	30763, 30800, 30626
Verbesserungen in der Übersicht der Systeminformationen. <ul style="list-style-type: none"> • Verbesserte Anzeige von Empfehlungen für Einstellungen und Hervorhebung kritische Werte. • Einige Eigenschaften des Datenbankservers für die Übersicht der Systeminformationen werden abhängig vom Konfigurationsparameter QBM DBServerProperties durch den DBQueue Prozessor ermittelt. 	30896, 30678, 30850
Verbesserte Protokollierung in der Prozesskomponente <code>MailComponent</code> .	31043
Release Management Unterstützung. Neuer Typ Release für Änderungskennzeichen zur Zusammenfassung von Änderungskennzeichen zu einem Release und zusätzliche Berichte im Designer.	29119
Aktualisierung des One Identity Redistributable STS auf die Version 2019.1.1.11.	30981
Der Report Editor verwendet Stimulsoft Ultimate 2019.1.1.	769216, 30873

Verbesserung	Fehler ID
Performanceoptimierung bei der Nachnutzung von String-Instanzen.	30341
Wird für die Datenübernahme in eine One Identity Manager History Database bereits ein Verbindungsserver bereitgestellt, wird dieser jetzt genutzt. Um diese Funktion zu nutzen, aktivieren Sie in der One Identity Manager History Database den Konfigurationsparameter HDB UseNamedLinkedServer und tragen Sie den Verbindungsserver in der One Identity Manager History Database als Server für die Quelldatenbank ein.	30028
Fehlermeldungen aus der Prozesshistorie werden in die One Identity Manager History Database übertragen.	29147
Verbesserte Protokollierung von Fehlermeldungen bei der Datenübernahme in die One Identity Manager History Database.	30165
Performanceverbesserung bei der Aktualisierung der One Identity Manager-Datenbank.	30292
Das Skript VID_FindAndReplaceByLine wurde gelöscht.	30632
Implementierung eines Lade-Cache <code>ISession.QueryCacheBlock()</code> um SQL-Abfragen, die potentiell mehrfach aufgerufen werden können, in einem Block zu laden.	27856, 29705
Verbesserter Schutz vor potentiell schädlichen SQL Ausführungen.	31299, 31301

Tabelle 2: Allgemein Webanwendungen

Verbesserung	Fehler ID
Performanceverbesserungen im Web Portal. <ul style="list-style-type: none"> • beim Anzeigen von Delegierungen, zu genehmigenden Bestellungen und der Bestellhistorie • beim Verarbeiten von Anfragen zu Attestierungsvorgängen • beim Ermitteln aller Berechtigungen einer Person • beim Genehmigen von Bestellungen 	770382, 29414, 30470, 30471, 30673, 30863, 31192
Auf der Anmeldeseite kann bereits vor der Anmeldung die Sprache eingestellt werden.	781956
Web Portal Benutzer können bereits bei der Registrierung ihre bevorzugten Spracheinstellungen festlegen.	795283
Wenn die erste Anmeldung am Web Portal scheitert, weil beispielsweise der Bestätigungslink abgelaufen ist, kann eine neue Bestätigungs-E-Mail angefordert werden.	30812
Verbesserte Benutzerführung im Web Portal.	726106,

Verbesserung	Fehler ID
<ul style="list-style-type: none"> Die Seite Verantwortlichkeiten Auditierung wurde strukturell überarbeitet. Die Anzeige einiger Parameter im Filterassistenten wurde benutzerfreundlicher gestaltet. Die Sortierung für Listen (DialogTree.ListOrderBy) wird in den Hyper-Views im Web Portal berücksichtigt. Die Detailansichten und Übersichtskacheln für Geschäfts- und Systemrollen zeigen mehr Informationen an. Die Anzeige von potentiellen Regelverletzungen wurde verbessert. Die Anzeige von URLs in Eigenschaftsansichten wurde verbessert. Die Seite Meine Vorgänge wurde überarbeitet und verbessert. Die Suche wird an weiteren Ansichten angeboten. Hyper-Views zeigen zusätzliche Informationen an. 	738158, 745500, 760498, 761671, 762208, 768037, 773368, 773566, 775573, 781813, 783457, 30034
<p>Verbesserte Benutzerführung bei der Bearbeitung und Genehmigung von Bestellungen.</p> <ul style="list-style-type: none"> Die Merkliste für Bestellungen kann mit einem Mausklick komplett gelöscht werden. Nach dem Verschieben des letzten Produktes aus der Merkliste in den Einkaufswagen, wird dem Benutzer automatisch der Warenkorb angezeigt. Nach dem Verschieben des letzten Produktes aus dem Einkaufswagen auf die Merkliste wird dem Benutzer automatisch die Merkliste angezeigt. In der Detailansicht der Bestellhistorie kann leichter zu Objekten navigiert werden, die mit der Bestellung zusammenhängen. Verbesserte Anzeige von Servicekategorien bei Bestellungen. Klickt ein Benutzer auf den E-Mail-Link zur Entscheidung über eine Bestellung und es wurde bereits über diese Bestellung entschieden, wird dies dem Benutzer durch eine entsprechende Benachrichtigung im Web Portal mitgeteilt. Die Seite Bestellungen für <Benutzer> bietet eine Empfängerauswahl an, falls eine Bestellung mehrere Empfänger hat. Die Ansicht zu genehmigender Bestellungen ist nun nach der Priorität sortiert. Die Information zum Zeitpunkt einer Bestellung in der Bestellhistorie ist übersetzbar. In den Bestellübersichten kann nach der Bestellung sortiert und gefiltert werden. 	738155, 738157, 740766, 746966, 769201, 769896, 775198, 784674, 786514, 794762, 795801

Verbesserung	Fehler ID
<ul style="list-style-type: none"> Die Auswahl, die festlegt, welche Bestellungen kopiert, nochmal abgesendet oder in eine Bestellvorlage übernommen werden können, wurde überarbeitet. 	
Beim Bestellen von Produkten wird angezeigt, ob das Produkt bereits bestellt wurde. Produkte, die bereits bestellt wurden, können nicht mehr in den Einkaufswagen gelegt werden.	736902, 25756
Wenn eine kundenspezifische Bestelleigenschaft mit einer Standard-eigenschaft von Bestellungen identisch ist (beispielsweise das Gültig von-Datum), wird im Einkaufswagen nur die kundenspezifische Bestelleigenschaft angezeigt.	29305, 743621
Die Prüfung, welche Personen ein Produkt bestellen dürfen, wurde auf die Tabelle AccProductInDepartment erweitert.	748251
Mit dem neuen Web Designer Konfigurationsparameter VI_ITShop_Employee_Preselected kann festgelegt werden, ob der angemeldete Benutzer immer als Empfänger einer neuen Bestellung vorausgewählt wird.	748875
Der Standardwert für die Verlängerung einer Bestellung ist nun ein Wert in der Zukunft und mithilfe des Web Designer Konfigurationsparameters VI_ITShop_Prolongation_Offset konfigurierbar.	738195, 26139
<p>Verbesserte Benutzerführung bei der Attestierung mit automatischem Entzug von Berechtigungen.</p> <ul style="list-style-type: none"> Die Mailvorlagen enthalten einen Link zu den Details des Attestierungsvorgangs und einen Warnhinweis, wenn durch eine negative Attestierung Berechtigungen automatisch entzogen werden. Dem Attestierer werden verschiedene Details zu den Berechtigungen angezeigt, welche bei einer negativen Attestierung entzogen werden. 	736904, 794742, 30893
Web Portal Benutzer können die Details aller sie betreffenden Attestierungsvorgänge sehen.	30325
Neuer Tabreiter Compliance auf der Seite Offene Attestierungen . Es werden detaillierte Informationen über Regelverletzungen des zu attestierenden Objekts angezeigt.	783486
Wenn an einer Rolle die Option Keine Vererbung an Personen aktiviert ist, wird bei der Complianceprüfung von Bestellungen dieser Rolle oder bei Direktzuweisung auf potentielle Regelverletzungen hingewiesen. Die Regeln werden verletzt, sobald die Option Keine Vererbung an Personen deaktiviert wird.	760181, 25477
Beim Auflösen von Regelverletzungen werden auch SAP Rollen berücksichtigt, die SAP Funktionen treffen.	782806
Wenn bei der Auflösung von Regelverletzungen auf der ersten Seite keine	787292

Verbesserung	Fehler ID
Berechtigungen gefunden werden, wird nun ein besserer Fehlertext angezeigt.	
Benutzer mit der Anwendungsrolle Identity Management Personen Administratoren können nun auch im Web Portal Personen administrieren.	715356
Bei der Auswahl von Personen oder Benutzerkonten wird auch deren Identität angezeigt.	28878
Der Filterassistent wird nur für Benutzer mit der Programmfunktion Erlaubt die Nutzung des SQL Assistenten im Web Portal (Common_SqlWizardWeb) angezeigt.	792338, 30240
In Tabellen, die hierarchische Objekte anzeigen, wird die Anzahl der Einträge auf oberster Ebene angezeigt.	758936
Einzelne Teile von Hyper-Views können im Web Portal ausgeblendet werden.	764013
Die Sitzung im Web Portal kann nun über eine feste URL /page.axd?ContextID=QBM_Logout geschlossen werden.	771671
Fehlende Formularmethoden wurden bisher als Fehler im Protokoll vermerkt. Da es im Normalbetrieb zu vielen falschen Fehlermeldungen aufgrund von sich zeitlich überschneidenden Benutzeraktionen kommt, werden diese Fehler nun ignoriert.	30373
Einige Fehlermeldungen bieten jetzt Lösungsvorschläge zu Fehlern an.	785123
Mit dem neuen Web Designer Konfigurationsparameter VI_Common_AutoCompleteListCount kann festgelegt werden, wie viele Treffer für die Autovervollständigung angezeigt werden.	670646
Mit dem neuen Web Designer Konfigurationsparameter VI_Common_HyperView_DisableNavigation kann die Navigation zu anderen Objekten für alle Hyper-Views deaktiviert werden.	779809
Mit dem neuen Web Designer Konfigurationsparameter VI_Common_AutoCompletePrefixOnly kann für die Autovervollständigung in Eingabefeldern festgelegt werden, ob nur Treffer angezeigt werden, die mit dem eingegebenen Begriff beginnen oder diesen an beliebiger Stelle enthalten.	780465
Mit dem neuen Web Designer Konfigurationsparameter VI_Common_CaptchaCaseInsensitive kann festgelegt werden, ob die Groß-/Kleinschreibung bei der Eingabe des Captchas geprüft wird.	785849
Am Kennwörterücksetzungsportal können sich auch Personen anmelden, die im System als inaktiv mit Zertifizierungsstatus neu vermerkt sind.	30742
Verbesserte Benutzerführung im Kennwörterücksetzungsportal. <ul style="list-style-type: none"> Die Rückkehr zur Startseite ist jederzeit möglich. 	724499, 759436, 789656,

Verbesserung	Fehler ID
<ul style="list-style-type: none"> • Auf der Anmeldeseite lässt sich bereits vor der Anmeldung die Sprache einstellen. • Kennwortfragen und -antworten können auch im Kennwortrücksetzungsportal gesetzt und geändert werden. • Benutzer können auch die Kennwörter ihrer Subidentitäten im Kennwortrücksetzungsportal ändern. 	794857
Im Web Portal für Betriebsunterstützung kann die Suche nach Objekten auf bestimmte Tabellen eingeschränkt werden.	772962
<p>Verbesserte Benutzerführung im Web Designer.</p> <ul style="list-style-type: none"> • Das Design wurde überarbeitet. • Das Hilfe-Menü wurde überarbeitet. • Begrifflichkeiten zur Projektspeicherung wurden geändert. Statt Speicherart wird nun Projekttyp verwendet. • Die Suchfunktion wurde in der englischen Oberfläche in Find umbenannt. • Die Information zum aktuellen Objekt wird jetzt in der Symbolleiste statt in der Knotenbearbeitung angezeigt. 	771460, 781812, 785007, 786212, 787063
Am Knoten für die Baumebene wurde eine neue Eigenschaft eingefügt, die steuert, welche Knoten automatisch beim Laden ausgeklappt werden sollen.	789080
Es ist jetzt möglich, aus einem Bericht direkt zu den Übersichtsseiten der einzelnen Einträge zu springen.	691041
Die Funktion EditFilter() an der Web Designer Komponente VI_Edit_LimitedValues wurde entfernt. Einschränkungen der erlaubten Werte müssen über Erweiterungen vorgenommen werden.	787115
Die Web Designer Komponente VI_Audit_Responsibilities nutzt für die Anzeige die Datenbanksicht TSBVUNSRoot.	763281
Aus dem Web Designer kann nun auch Microsoft Edge gestartet werden.	750375
Objektabhängige Verweise können im Web Designer bearbeitet und deaktiviert werden.	753696, 753699, 29313
Das Skript zur Statusanzeige für Menüeinträge (DialogTree.StateScript) wird auch vom Web Designer berücksichtigt.	29989
Kommentare können nun direkt oder per Extension an Collections hinzugefügt werden.	709434
Der Web Designer Configuration Editor prüft nun, ob ein Benutzerkonto für die automatische Aktualisierung vorhanden ist und die Zugangsdaten korrekt	736495

Verbesserung	Fehler ID
sind. Ist dies nicht der Fall, so kann man ein neues Benutzerkonto erstellen.	
Änderungen an Dateien, die außerhalb des Web Designers durchgeführt wurden, werden jetzt nicht mehr durch das Speichern im Web Designer überschrieben.	762527
Die Meldungen des Web Designer-Compilers können anhand von Fehlercodes besser identifiziert werden. Zudem kann man festlegen, welche Warnungen als Fehler behandelt werden sollen und welche Fehlercodes ignoriert werden sollen.	780370, 780371
Die Anzeige der Protokolldateien im Web Portal Monitor wurde überarbeitet.	741876
In der Protokolldatei der Webanwendung werden die IDs der ausgeführten Web Designer Knoten ausgegeben.	766259
Direkte HTTP-Aufrufe zur Starling 2FA API sind jetzt nicht mehr möglich. Die QER.DefenderClient.dll wurde in QER.Starling2FAClient.dll umbenannt.	720212
Die Starling 2FA Client API Version 5.9.18078.3 wird unterstützt. Angepasste Skripte: QER_CreateMFAUserID und QER_DeleteMFAUserID	767068, 770670
Um eine Cross-Site-Request-Forgery (CSRF) zu vermeiden, wird bei der Installation des Web Portals das Attribut SameSite für Cookies mit dem Wert strict vorbelegt.	777728
Um mehr Sicherheit zu gewährleisten, wurde die standardmäßig installierte Datei web.config um den Parameter httpRuntime enableVersionHeader="false" erweitert.	736623
AngularJS 1.7.2 wird verwendet.	774246
Verwendet der Benutzer eine Benutzeroberfläche mit hohem Kontrast, werden ausgewählte Einträge in Tabellen durch einen Rand hervorgehoben.	738193

Tabelle 3: Zielsystemanbindung

Verbesserung	Fehler ID
Veraltete Synchronisationsrevisionen werden innerhalb der täglichen Wartungsaufträge aus der Tabelle DPRRevisionStore gelöscht.	22602
Die Wartung des Synchronisationspuffers kann im Expertenmodus des Synchronization Editor manuell ausgeführt werden.	24438
Optimierung des Datendurchsatzes bei der Provisionierung, wenn ein Anwendungsserver eingesetzt wird.	27347
Beim Erstellen eines Synchronisationsprojekts aus einer benutzerdefinierten Projektvorlage werden die Einzelobjektoperationen für die Provisionierung und Einzelobjektsynchronisation durch den Projektassistenten angelegt.	28280
Verbesserte Darstellung von ausstehenden Mitgliedschaften von Objekten	28491,

Verbesserung	Fehler ID
auf den Überblicksformularen für Zielsystemobjekte.	19817
Die Einzelprovisionierung kann auch mit Wertevergleichsregeln, die mehrwertige Schemaeigenschaften mappen, umgesetzt werden.	28759
An Schemaeigenschaften zur Schlüsselauflösung kann konfiguriert werden, ob nicht-auflösbare Schlüssel im Synchronisationsprotokoll aufgezeichnet werden sollen.	29092
Schemaeigenschaften für die Schlüsselauflösung können als Nur lesend definiert werden.	29171
Die Zuordnung eines Managers an eine Person kann bei der Synchronisation einer Oracle E-Business Suite entfernt werden. Die Zuordnung eines Managers an eine Abteilung kann bei der Synchronisation mit einem SAP HCM System entfernt werden.	29265
Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#29265 bereitgestellt.	
<p>Verbesserte Benutzerführung im Synchronization Editor:</p> <ul style="list-style-type: none"> • Verbesserte Darstellung von Mitgliederlisten im Zielsystembrowser. Die im Bearbeitungsdialog einer Schemaeigenschaft angezeigten Objekte können sortiert werden. • Es werden detaillierte Informationen zu den Ergebnissen der Konsistenzprüfung angezeigt. • Wenn im Synchronization Editor ein Synchronisationsprojekt geöffnet wird, erscheint eine Meldung, wenn ein anderer Benutzer dieses Synchronisationsprojekt bereits bearbeitet. • Beim Aktivieren und Speichern bereits aktivierter Synchronisationsprojekte wird die Konsistenzprüfung automatisch durchgeführt. Sind Fehler enthalten, wird nachgefragt, ob das Synchronisationsprojekt aktiviert beziehungsweise gespeichert werden soll. • Verbesserte Darstellung des Scopes im Synchronization Editor. • Verbesserungen im Dialog Systemverbindung auswählen beim Erstellen eines Synchronisationsprojekts. • Im Zielsystembrowser kann der Filter zum Anzeigen der Ergebnisliste für den ausgewählten Schematyp bereits vor dem Laden der Liste definiert werden. 	24317, 29258, 29334, 29363, 29396, 29957, 30197
<p>Neue Konsistenzprüfungen wurden implementiert.</p> <ul style="list-style-type: none"> • Prüfung von Property-Mapping-Regeln • Prüfung, ob Startkonfigurationen, die zu einer Startgruppe zusammengefasst wurden, denselben Zeitplan verwenden. 	29642, 30654, 30780

Verbesserung	Fehler ID
<ul style="list-style-type: none"> Prüfung, ob Schemaeigenschaften verwendet werden, die intern als obsolet gekennzeichnet wurden. 	
Verbesserte Fehlermeldung, wenn ein Synchronisationsprojekt nicht geöffnet werden kann, weil verwendete Skripte Syntaxfehler enthalten.	29947
Im Zielsystembrowser können Systemobjekte dargestellt werden, die verschlüsselte Werte enthalten.	30021
Synchronisationsprojekte können automatisiert aktualisiert werden. Die Konfigurationsdatei kann über ein Referenzprojekt bereitgestellt werden.	30416
An Skripteigenschaften kann konfiguriert werden, ob Fehler beim Ausführen des Skripts ignoriert werden sollen.	30591
Performanceverbesserungen <ul style="list-style-type: none"> bei der Einzelprovisionierung von Mitgliedschaften bei der Berechnung von DBQueue Prozessor-Aufträgen bei der Synchronisation bei der Provisionierung von neuen Objekten mit Windows PowerShell-basierten Konnektoren 	22556, 29063, 30667, 30702, 30864, 30892, 30922, 30942
Synchronisationsprotokolle werden auch im Manager angezeigt.	30949
Zusätzliche Objektdefinition für die Anzeige von Benutzerkonten im Manager abhängig von der jeweiligen Identität.	27038
An Active Directory Standorten wird die Beziehung zur Gesamtstruktur abgebildet. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#29306 bereitgestellt.	29306
Die Optionen Kennwort läuft nie ab und Kennwort bei der nächsten Anmeldung ändern an Active Directory Benutzerkonten können nicht mehr gleichzeitig aktiviert werden.	30521
Bei der Synchronisation von Active Directory Benutzerkonten werden die Verweise auf Cloud Benutzerkonten synchronisiert. Die Synchronisation wird durch Active Directory Konnektor und den Active Roles Konnektor unterstützt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#29087 bereitgestellt.	29087
Bei der Synchronisation mit dem Active Roles Konnektor werden Informationen zum Betriebssystem von Active Directory Computern eingelesen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#28612 bereitgestellt.	28612

Verbesserung	Fehler ID
Der Azure Active Directory Konnektor verwendet Microsoft Graph .NET Wrapper Version 1.6.2.	28801
Der Konfigurationsparameter TargetSystem AzureAD ist ein präprozessorrelevanter Konfigurationsparameter.	30485
Microsoft Exchange Raumpostfächer können für aktive Active Directory Benutzerkonten erstellt werden.	28222
Der Postfachtyp von Microsoft Exchange Postfächern kann geändert werden.	30569
Für Remotepostfächer können Proxyadressen verwaltet werden.	29949
Es können Remotepostfächer mit dem Postfachtyp Remote freigegebenes Postfach erstellt werden.	30252
Beim Aktivieren eines Postfachs wird geprüft, ob bereits ein Remotepostfach oder ein E-Mail-Benutzer für das angegebene Active Directory Benutzerkonto existiert.	31126
Nicht mehr benötigte Property-Mapping-Regeln wurden aus dem Mapping OwaMailboxPolicy entfernt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30498 bereitgestellt.	30498
Buchungsberechtigungen für Exchange Online Raumpostfächer und Gerätepostfächer können jetzt auch für dynamische Verteilergruppen, E-Mail aktivierte Verteilergruppen und Office 365 Gruppen erteilt werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30588 bereitgestellt.	30588
Die Liste der Fehlermeldungen, anhand derer ein Verbindungsabbruch angenommen wird, wurde erweitert um die Meldungen: An error caused a change in the current set of domain controllers. Your request is too frequent. Please wait for few minutes and retry. Topology Provider coundn't find the Microsoft Exchange Active Directory Topology service on end point.	31168
Performanceverbesserung bei der Synchronisation von Exchange Online Empfängerlisten.	30959, 31162
Es werden auch die primären Mitgliedschaften von Personen in Standorten synchronisiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#29741 bereitgestellt.	29741
Im Systemverbindungsassistenten werden Schemaerweiterungsdateien für Oracle E-Business Suite auch auf funktionale Fehler überprüft.	30402

Verbesserung	Fehler ID
<p>Beim Einrichten der Synchronisation mit einer E-Business Suite kann die Oracle Database Edition ausgewählt werden. Die Edition kann im Verbindungsparameter jederzeit geändert werden.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30464 bereitgestellt.</p>	30464
<p>Das Serialisierungsformat an den Schematypen in Synchronisationsprojekten für eine Oracle E-Business Suite wurde geändert.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31011 bereitgestellt.</p>	31011
<p>Für die Synchronisation einer G Suite-Umgebung kann ein nur lesender API-Zugriff konfiguriert werden.</p>	29934
<p>Im Manager kann die Eigenschaft Vererbung blockieren an G Suite Organisationen (GAPOrgUnit.BlockInheritance) nicht mehr bearbeitet werden, da sie mit der Google Admin-Konsole ebenfalls nicht bearbeitet werden kann. Diese Eigenschaft sollte nicht mehr genutzt werden.</p>	30452
<p>Der G Suite Konnektor nutzt Google.Apis Version 1.37.0.</p>	30979
<p>Möglichkeit zur Umdefinition von strukturellen Klassen zu Auxiliary-Klassen im LDAP Konnektor.</p>	20824
<p>Leerzeichen in den definierten Namen von LDAP Objekten werden toleriert.</p>	30542, 30543
<p>Die automatische partitionierte Suche für LDAP Server mit Oracle Directory Server Enterprise Edition (ODSEE) wird nicht mehr unterstützt. Die partitionierte Suche kann im Systemverbindungsassistenten konfiguriert werden. Dazu wählen Sie auf der Seite Einstellungen für partitionierte Suche die Objektklasse nsUniqueId und verwenden Sie als Zeichen ABCDEF0123456789.</p>	30733
<p>Beim Anlegen von Notes Postfachdateien kann die Zugriffsstufe für den Besitzer gesetzt werden. Welche Zugriffsstufe standardmäßig übergeben wird, ist im Konfigurationsparameter TargetSystem NDO Accounts MailFileAccessRole festgelegt.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30313 bereitgestellt.</p>	30313
<p>Performanceverbesserungen</p> <ul style="list-style-type: none"> • bei der Provisionierung von Notes Objekten • bei der Synchronisation von Notes Gruppenmitgliedschaften 	30658, 30895
<p>An die Prozessfunktion RunAgent aus der Prozesskomponente NDO Component können jetzt Parameter vom Typ IN übergeben werden.</p>	30856

Verbesserung	Fehler ID
Das Kommunikations-Timeout zwischen SharePoint Konnektor und Zielsystem wurde auf 24 Stunden angehoben.	30804
Der Konfigurationsparameter TargetSystem SharePoint Online ist ein präprozessorrelevanter Konfigurationsparameter.	30486
SAP Benutzerkonten können im One Identity Manager umbenannt werden. Dabei werden die Eigenschaften des Benutzerkontos auf ein neues Benutzerkonto übertragen und das bisherige Benutzerkonto wird gelöscht.	29285
Im Systemverbindungsassistenten werden Schemaerweiterungsdateien für SAP R/3 auch auf funktionale Fehler überprüft.	30304
<p>Performanceverbesserungen</p> <ul style="list-style-type: none"> • bei der Berechnung von SAP Funktionen • bei der Berechnung der Hierarchien von SAP Gruppen, Rollen und Profilen • bei der Synchronisation von Rollenzuordnungen mit dem Zentralsystem einer ZBV (UserInCUARole) <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30941 bereitgestellt.</p>	30299, 30743, 30675, 30941
Die Prozesskomponente SAP Component wurde um die Prozessfunktionen ObjectExists und DelRoleFromUser erweitert.	31120, 31145
Der SCIM Konnektor kann Clientzertifikate zur Authentifizierung nutzen.	30154
Die bei der Synchronisation verwendeten Variablen und deren Werte werden protokolliert.	30190
<p>In Synchronisationsprojekten mit dem SCIM Konnektor kann die Verwendung des lokalen Caches konfiguriert werden.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30497 bereitgestellt.</p>	30497
Der CSV Konnektor erkennt mehrfache identische Einträge in der CSV-Datei. Bei der Synchronisation kann ein Eintrag ausgewählt werden oder alle Einträge werden ignoriert.	30716
Erweiterte Konsistenzprüfungen im Windows PowerShell Konnektor.	29201, 30220
Wird im Windows PowerShell Konnektor ein Verbindungsabbruch erkannt, wird bei jedem Wiederverbindungsversuch auch die Fehlermeldung per NLog ausgegeben, die zum Verbindungsabbruch führte.	31164

Tabelle 4: Identity Management und Access Governance

Verbesserung	Fehler ID
<p>Vereinfachte Unterstützung des Sonderprozesses zum Löschen von Personen bei der Umsetzung der Datenschutz-Grundverordnung (DSGVO).</p> <ul style="list-style-type: none"> • Es wird eine neue Prozedur QER_PPersonDelete_GDPR bereitgestellt. • Die Prozessfunktion Delete der Prozesskomponente HandleObjectComponent besitzt einen neuen Parameter Deep zum Löschen abhängiger Objekte und Referenzen. 	27643, 30468, 30721
Der Delegierende kann über die Entscheidung benachrichtigt werden.	20893
Wenn Mitgliedschaften in Rollen und Organisationen attestiert werden (Tabelle PersonInBaseTree), kann jetzt auch das Entscheidungsverfahren CM zur Ermittlung der Attestierer genutzt werden.	30123
Wenn an einer Attestierungsrichtlinie das Attestierungsverfahren geändert wird, wird geprüft, ob die bereits zugeordnete Entscheidungsrichtlinie dafür zugelassen ist.	30218
Es kann konfiguriert werden, welche Methode auf Bestellungen ausgeführt wird, wenn bei einer negativen Attestierung die bestellte Zuweisung entfernt werden soll. Neuer Konfigurationsparameter: QER Attestation AutoRemovalScope PWOMethodName	30581
Das Entscheidungsverfahren OA kann auch zur Ermittlung der Attestierer genutzt werden, wenn Zuweisungen von Systemberechtigungen an Benutzerkonten oder Zuweisungen von Systemrollen an Personen attestiert werden sollen.	30636
Neues Entscheidungsverfahren zur Ermittlung von Attestierern für Benutzerkonten: EA - Person des Benutzerkontos.	30871
An Standardbegründungen können Nutzungstypen zugeordnet werden. Im Web Portal werden die Standardbegründungen darüber gefiltert. Bei der Aktualisierung des One Identity Manager werden den kundenspezifischen Standardbegründungen alle Nutzungstypen zugeordnet. Diese Zuordnungen können im Manager bearbeitet werden.	22810, 789946
Es kann am Entscheidungsschritt festgelegt werden, ob Personen, die von der Entscheidung betroffen sind, diesen Entscheidungsschritt entscheiden dürfen. Damit kann verhindert werden, dass	24141
<ul style="list-style-type: none"> • der Besteller und der Empfänger einer Bestellung über die Bestellung entscheiden, • die zu attestierende Person den Attestierungsvorgang entscheidet. 	
Standard-Entscheidungsverfahren können für kundenspezifische Anpassungen kopiert werden.	24176

Verbesserung	Fehler ID
An Entscheidungsrichtlinien können jetzt auch Mailvorlagen für Verlängerung und Abbestellung zugeordnet werden. Der Konfigurationsparameter QER ITShop MailTemplateIdents InformRecipientAboutUnsubscribe wurde gelöscht.	27142
Neue Mailvorlagen für Benachrichtigungen bei Delegation einer Entscheidung. Zur Konfiguration dieser Benachrichtigungen wurden neue Konfigurationsparameter unter QER ITShop Delegation MailTemplateIdents eingeführt.	27349
Bestellte Zuweisungen von Unternehmensressourcen an Geschäftsrollen und Organisationen können erhalten bleiben, wenn der Empfänger der Bestellung aus dem Kundenknoten entfernt wird. Zur Konfiguration dieses Verhaltens wurden neue Konfigurationsparameter unter QER ITShop ReplaceAssignmentRequestOnLeaveCU eingeführt.	27640
Performanceverbesserung bei der Berechnung von Delegationen.	28964
Bereits bei der Bestellung im IT Shop erzeugt die Methode CreateITShopOrder einen Eintrag im Entscheidungsverlauf.	30368
Die Aufgabe Entfernen aus allen Regalen wird nur angezeigt, wenn die Unternehmensressource einem IT Shop Regal als Produkt zugewiesen ist.	30382
Im Konfigurationsparameter QER ITShop LimitOfNodeCheck ist festgelegt, wie viele Produktknoten in einem DBQueue Prozessor-Lauf gelöscht werden sollen, wenn durch automatische Prozesse massenhaft Produkte im IT Shop gelöscht werden. Standardmäßig werden 500 Objekte in einem Lauf verarbeitet. Falls Performanceprobleme bei der Ausführung des Auftrags QER-K-OrgAutoChild auftreten, stellen Sie einen niedrigeren Wert ein.	30657
Ungenutzte Anwendungsrollen für Produkteigner werden jetzt auch dann gelöscht, wenn der Konfigurationsparameter QER ITShop GroupAutoPublish deaktiviert ist.	30796
Performanceverbesserung bei der Bestellprozessverarbeitung.	30990
Verbesserungen bei der Vererbungsberechnung für Systemrollen. <ul style="list-style-type: none"> • Neuer Konfigurationsparameter für die Definition von sich ausschließenden Systemrollen: QER Structures Inherit ESetExclusion. • Sonderbehandlung, wenn Systemrollen über hierarchische Rollen vererbt werden. Neuer Konfigurationsparameter: QER Structures Inherit NoESetSplitting 	28248, 28973
Auf dem Überblicksformular für eine Systemrolle werden Unternehmensressourcen, die über untergeordnete Systemrollen zugewiesen sind, in separaten Formularelementen angezeigt.	30737

Verbesserung	Fehler ID
Beim Festlegen der betroffenen Berechtigungen in der Regelbedingung von Compianceregeln können die Teilbedingungen Hat Zusatzeigenschaft aus Gruppe und SQL Abfrage definiert werden.	29100
Verbesserte Darstellung von Regelverletzungen mit Beteiligung von SAP Funktionen. <ul style="list-style-type: none"> • Neues Überblicksformular mit Details zur Regelverletzung einer Person, den verantwortlichen Objekten und den zugewiesenen risikomindernden Maßnahmen. • Auf den Überblicksformularen für SAP Benutzerkonten, SAP Rollen und SAP Profilen, Geschäftsrollen und Organisationen werden getroffene SAP Funktionen angezeigt und die Compianceregeln, welche dadurch verletzt werden können. • Auf dem Überblicksformular einer SAP Funktionsausprägung werden verletzte Compianceregeln und betroffene Geschäftsrollen und Organisationen angezeigt. 	29376
An Personen kann ein Mitarbeitertyp angegeben werden. Damit wird die Beziehung der Person zum Unternehmen dargestellt.	787290, 29094
Berichte über Personen enthalten zusätzliche Informationen.	30063, 30079
Wenn die Option Zeitweilig deaktiviert an einer Person deaktiviert wird und das Datum für Zeitweilig deaktiviert ab in der Zukunft liegt, wird das Datum für Zeitweilig deaktiviert ab und Zeitweilig deaktiviert bis nicht mehr gelöscht.	30344
Wenn eine dauerhaft deaktivierte Person erneut aktiviert wird, werden das Austrittsdatum und das Datum des letzten Arbeitstages nur noch dann gelöscht, wenn es in der Vergangenheit liegt.	30993
Rollentypen können an Rollenklassen zugewiesen werden. Damit kann die Verwendung der Rollentypen auf die zugewiesenen Rollenklassen eingeschränkt werden.	28131
An Anwendungsrollen können ein Manager und ein zweiter Verantwortlicher zugeordnet werden.	29228
Performanceverbesserung bei der Ermittlung der Eigentümer von Systemberechtigungen.	30223

Siehe auch:

- [Schemaänderungen](#) auf Seite 49
- [Patches für Synchronisationsprojekte](#) auf Seite 58

Gelöste Probleme

Nachfolgend finden Sie eine Liste von in dieser Version behobenen Problemen.

Tabelle 5: Allgemein

Gelöstes Problem	Fehler ID
Wenn sowohl in der One Identity Manager-Datenbank als auch in der History Database Prozessanzeigen mit identischer Prozessgruppen ID vorhanden sind, schlägt die Befüllung der Raw-Tabellen fehl.	27846
Fehler bei der Befüllung der Raw-Tabellen, wenn die One Identity Manager-Datenbank und die History Database im gleiche SQL-Cluster installiert sind.	30455
Bei der One Identity Manager History Database-Installation werden der One Identity Manager History Service und der One Identity Manager Service gleichzeitig installiert. Zur Behebung des Problems wurde die Datei HDBService.exe entfernt. Die Installation des Dienstes für eine History Database erfolgt jetzt über die Datei viNetworkService.exe.	28058
i WICHTIG: Wenn Sie von diesem Problem betroffen sind, deinstallieren Sie vor der Aktualisierung Ihrer One Identity Manager History Database-Installation den One Identity Manager History Service. Führen Sie in der Kommandozeile im administrativen Kontext folgenden Aufruf aus: <code>sc delete "HDBService"</code>	
Fehler beim Prüfen von E-Mail-Adressen auf Eindeutigkeit, wenn eine E-Mail-Adresse durch eine Bildungsregel neu berechnet wurde, der alte und der neue Wert jedoch identisch sind.	30300
Für Spalten, die Teil eines Primärschlüssels oder Teil des Schlüssels einer M:all-Tabelle sind, können Bearbeitungsrechte gesetzt werden.	29031
Fehlermeldung beim Aufruf der Quantum.MigratorCmd.exe mit der Operation DUMP.	30305
Probleme beim Öffnen des Wörterbucheditor im Designer, wenn sehr große Tabellen zur Übersetzung geladen werden.	30319
Die Funktion QBM_FSQRemoveComment erkennt keine Linux-Zeilenwechsel.	30342
Das Skript zur Serverauswahl an einem Prozessschritt (Job.ServerDetectScript) wird nicht implizit um einen Try-Catch-Block erweitert.	30347
Behinderung der Auslieferung von Prozessschritten bei Massenoperationen durch Einträge in der Tabelle QBMElementAffectedByJob.	30362

Gelöstes Problem	Fehler ID
Wenn für eine Spalte des Objektes eine wechselseitige Beziehung mit einer anderen Spalte in der Tabelle <code>QBMColumTranslation</code> existiert, kommt es beim Laden eines solchen Objektes zum Absturz des Programms.	30380
Enthält ein Prozess oder ein Prozessschritt Anführungszeichen (") im Namen, scheitert die Kompilierung.	30403
Fehler bei der Anmeldung über einen Anwendungsserver, wenn der Benutzer mit türkischen Spracheinstellungen arbeitet.	30445
Session-ID im Anwendungsserver kann wiederverwendet werden.	31299, 31306
<p>i HINWEIS: Im Standard erfolgt jetzt keine Wiederverwendung der Session-ID.</p> <p>Die Verwendung der Session-ID ist konfigurierbar. In der Konfigurationsdatei des Anwendungsserver (<code>web.config</code>) wurde in der Sektion <code>server</code> ein neuer Parameter <code>allowsessionidreuse</code> eingefügt. Diese Änderung wirkt sich nur auf Neuinstallationen aus. Bestehende Installationen werden nicht geändert.</p> <p>Um die Wiederverwendung der Session-ID zu erlauben:</p> <ul style="list-style-type: none"> Für Neuinstallationen: Entkommentieren Sie den Parameter in der <code>web.config</code> des Anwendungsservers. Für bestehende Installation: Fügen Sie in der <code>web.config</code> des Anwendungsservers in der Sektion <code>server</code> folgenden Eintrag ein. <pre><add key="allowsessionidreuse" value="true" /></pre>	
Nach einem fehlgeschlagenen Transport befindet sich die Datenbank unter Umständen im Trigger-freien Zustand.	30459, 30447
Performanceprobleme bei der Ermittlung von Berechtigungen.	30471
Falscher Kurzname für Bundesland "Newfoundland and Labrador".	30484
Nach Schemaerweiterung von kundenspezifischen Tabellen vom Typ Read-Only sind die neuen Spalten mit der Option Durch Anwender konfigurierbar auf den Wert 0 gesetzt.	30491
Fehler in der Methode <code>SqlFormatter.NotInClause</code> .	30505
Probleme bei der Initialisierung der Jobqueue, wenn eine große Anzahl von Queues betroffen ist.	30539
Die physische Abhängigkeit zwischen DBQueue Prozessor Aufträgen wird für Aufträge ohne Parameter nicht beachtet.	30573
Die Erkennung von terminierten Slots ist fehlerhaft, wenn der SQL Server die SPID wiederverwendet.	30584

Gelöstes Problem	Fehler ID
Die Prozeduren zum Verkleinern der Einträge für die Tabellen DialogWatchOperation, JobHistory sowie DialogProcessChain verkleinern nicht blockweise.	30604
Bei der Übernahme von Änderungen in die Datenbank im Designer werden die Änderungszeiten in UTC angezeigt.	30610
Probleme bei der Ermittlung der resultierenden Berechtigungsfilter für Objekte.	30582, 31110
Die Migration entfernt nicht-lineare Abhängigkeiten nicht korrekt.	30693
Fehler bei Wiederholung von Prozessschritten mit dem Status MISSING .	30752
Die Prozedur QBM_PCustomSQLFill schlägt fehl mit der Meldung Violation of PRIMARY KEY constraint. Es wird eine neue Konsistenzprüfung Index name longer than 30 characters bereitgestellt.	30753
Die Customizer-Methode GetNextID schlägt bei Ausführung im Designer fehl.	30786
Kundenspezifische Spalten werden in der automatischen Vervollständigung bei der Eingabe von Skript-Code nicht berücksichtigt.	30805
Beim Kopieren eines Prozessschrittes im Prozesseditor wird die Definition der Priorität (Job.PriorityDefinition) nicht mit kopiert.	30903
Enthält die ID einer Jobdestination Sonderzeichen, funktionieren die Links auf der Statusseite des One Identity Manager Service nicht.	30924
Strg+C in der Ansicht Prozessschritt im Job Queue Info kopiert nicht die selektierten Werte.	30343
Job Queue Info wird unerwartet beendet, wenn ein Filter auf das Systemprotokoll gesetzt wird und der Filter viele Einträge zurückgibt.	30928
In Berichten werden IN-Klausel Abfragen auf UID-Spalten und XObjectKey-Spalten mit Unicode-Kennung ausgeführt.	30723
Bei Berichtabfragen wird das Limit für die IN-Klausel nicht korrekt beachtet.	30724
Blockierung der Weiterschaltung von Prozessen durch sehr häufiges Aufrufen der Prozedur QBM_PJobUpdateState.	30798
Fehler bei der Prozessverfolgung (NullReferenceException).	30978
Das Bundesland Florida ist der falschen Zeitzone zugeordnet.	31089
Die Prozedur ProcessShrink hinterlässt in der Tabelle DialogProcess Einträge mit BasisObjectType=<unknown Object>.	31007
Komponenten und Tasks mit MaxInstance=1 laufen durch Loadbalancing parallel.	29577

Gelöstes Problem	Fehler ID
Für DBQueue Prozessor Aufträge werden die Trigger zur Aufzeichnung von Änderungen an Konfigurationsdaten nicht generiert.	30646
Der One Identity Manager Service meldet die Prozessschritte zurück, die Slots bleiben jedoch blockiert.	31055

Tabelle 6: Allgemein Webanwendungen

Gelöstes Problem	Fehler ID
Fehler bei erneuter Anmeldung am Kennworrücksetzungsportal, wenn das Portal zeitweilig nicht genutzt wurde.	30423
Ungeeignete Fehlermeldung, wenn im Kennworrücksetzungsportal ein Kennwort eingegeben wird, das nicht der Kennwortrichtlinie entspricht.	29804
Eine Person kann die Mitgliedschaft in einer konkreten Geschäftsrolle mehrfach bestellen.	30194
Im Web Portal muss bei einer Delegierung für jeden Schritt die Schaltfläche Weiter zweimal angeklickt werden.	30216
Abbestellte Zuweisungsbestellungen werden in der Bestellhistorie angezeigt, obwohl die Option abgebrochen, abgelehnt oder abbestellt deaktiviert ist.	30726
Eine Bestellung der Standard-Leistungsposition Anlegen einer Active Directory Sicherheitsgruppe kann nicht genehmigt werden.	30837
Bei Anfragen zu Attestierungsvorgängen werden Pflichtfelder nicht geprüft.	30862
Wenn Modul Berichtsabonnement nicht installiert ist oder der Konfigurationsparameter QER RPS DefaultReportTemplate deaktiviert ist, wird im Web Portal trotzdem ein PDF-Export angeboten. Der Versuch ein PDF zu exportieren führt im Web Portal zum Fehler.	28160
Das Web-Browser-Control im Web Designer blockiert bestimmte URLs.	28626
Bei der Delegierung geht die Auswahl der Rollen verloren, wenn man zur Auswahl der Rollen die Seite wechselt.	29861
Bei der Indexsuche in M:N-Tabellen werden falsche Where-Klauseln generiert.	30679
Im Web Portal ist im Hinweis zu den Kennwortanforderungen die Zeichenklasse nicht übersetzt.	30960
Falsche Anzeigenamen für DialogSchedule.LastRun und DialogSchedule.NextRun im Zeitplaneditor.	30687
Im Web Portal wird bei der Auswahl einer Zuweisungsressource unter Verantwortlichkeiten die Kachel Mitgliedschaften angezeigt, obwohl an eine Zuweisungsressource keine Mitglieder zugewiesen werden können.	29440

Gelöstes Problem	Fehler ID
Diagramm-Seiten, die sich über mehrere Seiten erstreckten, werden fehlerhaft dargestellt.	737307
Fehler, wenn die Manager Webanwendung über einen Load Balancer aufgerufen wird.	31064
<p>HINWEIS: Im Standard ist das Anwenden der SameOrigin-Policy aktiviert, da es sich dabei um eine Sicherheitsfunktion handelt. Das Anwenden der SameOrigin-Policy kann jetzt optional abgeschaltet werden. Fügen Sie dazu in der Konfigurationsdatei der Manager Webanwendung (web.config) in der Sektion application folgenden Eintrag ein.</p> <pre><application> ... <add key="DoNotApplySameOriginPolicy" value="True" /> ... </application></pre>	
In der Konfigurationsdatei des Web Portals (web.config) ist noch die URL /AE.axd deklariert.	31299, 31302
Der Handler AE.axd für Session-Informationen wurde aus der Konfigurationsdatei des Web Portals (web.config) entfernt. Damit wird der Handler bei einem neu installierten Web Portal nicht mehr eingebunden. Ein bereits installiertes Web Portal ist von der Änderung nicht betroffen.	
<p>HINWEIS: Falls Sie den Handler noch benötigen und wieder einbinden möchten, fügen Sie in der Konfigurationsdatei des Web Portals (web.config) die folgenden beiden Zeilen ein:</p> <p>In der Sektion system.web\httpHandlers:</p> <pre><add verb="GET" path="AE.axd" type="VI.WebRuntime.Communication.ControllerRequestHandler, VI.WebRuntime" /></pre> <p>In der Sektion system.webServer\httpHandlers:</p> <pre><add name="AE.axd_GET" path="AE.axd" verb="GET" type="VI.WebRuntime.Communication.ControllerRequestHandler, VI.WebRuntime" /></pre>	

Tabelle 7: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Fehler beim Publizieren von Gruppenmitgliedschaften, wenn es Mitgliedereigenschaften gibt, die nicht gemappt sind.	29691
Fehler beim Ausführen des Skripts DPR_GetAdHocData.	29847

Gelöstes Problem	Fehler ID
Bei einer Provisionierung, die mehrere Synchronisationsschritte eines Workflows ausführt, werden Property-Mapping-Regeln mit der Option Mapping gegen die Synchronisationsrichtung erzwingen nicht vollständig berücksichtigt.	29922
Bei Änderungen von Gruppeneigenschaften werden zu viele Nachberechnungsaufträge in die DBQueue eingestellt.	30076
Bei einer Datenbank mit verschlüsselten Verbindungsinformationen wird das Dialogfenster zur Eingabe dieser Informationen im Hintergrund geöffnet, wenn Patches angewendet werden.	30162
Im Manager werden Änderungen am Wert von IT Betriebsdaten nicht gespeichert.	30295, 30746
Fehler beim Öffnen von Stammdatenformularen für Objekte aus kundenspezifischen Zielsystemen, wenn kundenspezifische Spalten angezeigt werden.	30336
Mit der Prozedur QBM_PDeleteDeep ist es nicht möglich, ein Zielsystem aus der Datenbank zu entfernen.	30374
Die Einstellungen in einem Hierarchiefilter, der in eine Variable umgewandelt wurde, werden entfernt, wenn vom Synchronization Editor keine Verbindung zum Zielsystem aufgebaut werden kann.	30391
Dateien im temporären Verzeichnis des Synchronisationsbenutzers werden nicht gelöscht.	30396
Fehler beim Lesen von Daten aus Spalten mit dem Datentyp varbinary, wenn diese als Primärschlüssel oder Teil des Primärschlüssels verwendet werden.	30474
Fehler beim Laden von Synchronisationsprojekten.	30503
Fehler in der Provisionierung beim Dekodieren von XML Zeichen.	30525
Simulationsergebnisse enthalten nicht genügend Detailinformationen.	30550
Provisionierungsaufträge für Gruppenmitgliedschaften werden unter der falschen GenprocID zusammengefasst.	30565
Es werden maximal 1024 geänderte Mitgliedschaften pro Gruppe provisioniert.	30597
Bei der Referenzauflösung werden zu viele Spalten geladen.	30600
Beim Aufräumen der Tabelle DPRMembershipAction werden mitunter Einträge gelöscht, die noch benötigt werden.	30603
Bei der Synchronisation werden in der One Identity Manager-Datenbank Objekte gelöscht, die im Zielsystem nicht eindeutig sind.	30715
Die Abarbeitung von zielsystemspezifischen Aufträgen in der DBQueue wird	30773

Gelöstes Problem	Fehler ID
blockiert, wenn gleichzeitig Synchronisationen für dieses Zielsystem laufen.	
Die Provisionierung von Gruppenmitgliedschaften schlägt nicht fehl, wenn ein referenziertes Objekt nicht gefunden wird.	30787
Skriptvariablen werden bei jedem Zugriff neu berechnet.	30864
Bei der Synchronisation entstehen doppelte Objekte in der One Identity Manager-Datenbank, wenn diese in der Datenbank angelegt und provisioniert werden, während die Synchronisation läuft.	30957
Bei der Provisionierung von Mitgliedschaften nutzt der One Identity Manager das falsche Mapping.	31024
Beim Aktualisieren des Schemas und beim Transport eines Synchronisationsprojekts wird die Quotadefinition entfernt.	31098
Das Kennwort des Synchronisationsbenutzers wird in Protokolldateien unverschlüsselt ausgegeben.	31112
Beim Starten einer Synchronisation wird das Variablenset zu spät geladen.	31152
Nachberechnungsaufträge für ausstehende Objekte, die zurückgesetzt wurden, werden nicht ausgeführt.	31180
Fehlerhafte Behandlung von Domänen in Vertrauensstellung in Active Directory Synchronisationsprojekten. Die Projektvorlage wurde korrigiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30192 bereitgestellt.	30192
Domänenübergreifende Mitgliedschaften werden bei der Provisionierung nicht gelöscht.	30256
Active Directory Gruppenmitgliedschaften werden nicht provisioniert, wenn am Benutzerkonto die Objekt SID fehlt.	30509
Fehler bei der Verarbeitung von unauflösbaren Schlüsseln, während der Active Directory Synchronisation.	30552, 30811
Gelöschte Werte in den Spalten HomeDirectory und ProfilePath an Active Directory Benutzerkonten werden nicht provisioniert.	30561
Fehler bei der Berechnung von Active Directory Gruppenmitgliedschaften, wenn die primäre Gruppe des Benutzerkontos geändert wurde.	30826
Fehler bei der Synchronisation der Schemaeigenschaften ObjectKeyManager und Secretary von Active Directory Benutzerkonten. Die Synchronisation bricht ab, obwohl Bei Fehler fortsetzen konfiguriert ist.	30967
Timeout bei der Synchronisation von Azure Active Directory Gruppenmitgliedschaften.	31051

Gelöstes Problem	Fehler ID
Initialisierung des Globalen Kataloges muss nicht beim Verbindungsaufbau zum Active Directory erfolgen, sondern erst beim ersten notwendigen Zugriff.	31178
Es sind nicht alle Berechtigungen dokumentiert, die für die Synchronisation einer Microsoft Exchange-Umgebung benötigt werden.	29901
Wenn eine Microsoft Exchange Adressliste als ausstehend gekennzeichnet wird, werden die zugehörigen Adressbucheinträge nicht als ausstehend gekennzeichnet.	30400
Fehler beim Löschen von ausstehenden Microsoft Exchange Adressbucheinträgen.	30401
Wenn eine Microsoft Exchange Postfachdatenbank als ausstehend markiert wird, werden deren Zuweisungen an Server nicht als ausstehend markiert.	30466
Fehler bei der Provisionierung von gelöschten Microsoft Exchange Postfächern, wenn eine Löschverzögerung konfiguriert ist.	30807
Das Laden von Microsoft Exchange Datenverfügbarkeitsgruppen schlägt fehl, wenn alle beteiligten Server heruntergefahren sind.	31131
Die Verarbeitungsmethode MarkAsOutstanding fehlt im Synchronisationsschritt RoleAssignmentPolicy für Microsoft Exchange. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#28815 bereitgestellt.	28815
Fehler bei der Provisionierung von Exchange Online Postfächern. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31269 bereitgestellt.	31269
Der Prozess zur Provisionierung von Mitgliedschaften in E-Business Suite Berechtigungen wird immer wieder erneut in die Jobqueue eingestellt, wenn die ID des Benutzerkontos (Spalte UserID) nicht gesetzt ist.	30349
Datumswerte in Skripteigenschaften werden nicht in ein kulturunabhängiges Format konvertiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#28962_EBS bereitgestellt.	28962
Fehler beim Einrichten der Synchronisation mit einem LDAP Verzeichnis, wenn im Serverschema ein AttributeType in Hochkommas zurückgegeben wird.	30366, 30337
Der kanonische Name von LDAP Objekten wird nicht automatisch gebildet, wenn die Art der Synchronisation von Keine Synchronisation auf One Identity Manager geändert wird.	30398
Fehler beim Einrichten der Synchronisation mit einer IBM Notes-Umgebung,	30427

Gelöstes Problem	Fehler ID
wenn die Verbindung zum Domino-Server getestet wird.	
Die Synchronisation wird abgebrochen, wenn der FullName eines Notes Dokuments nicht gelesen werden kann.	30691
Die Personendokumente von neu angelegten Notes Benutzerkonten erscheinen nicht in der Standardansicht des Adressbuchs.	30814
Fehler beim Synchronisieren von Notes Schablonen.	30907
Fehler beim Umbenennen eines Notes Benutzerkontos, wenn eine organisatorische Einheit zugeordnet ist.	30953
Fehler beim Anlegen eines gruppenbasierten SharePoint Online Benutzerkontos.	30729
Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30729 bereitgestellt.	
Die Verarbeitungsmethode MarkAsOutstanding fehlt in einigen Synchronisationsschritten für SAP R/3 Berechtigungsobjekte.	29477
Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#29477 bereitgestellt.	
Im One Identity Manager Administrationshandbuch für das SAP R/3 Compliance Add-on fehlt der Hinweis, dass die Synchronisation von SAP Berechtigungsobjekten für die Mandanten einer Zentralen Benutzerverwaltung nicht unterstützt wird.	29676
An SAP Benutzerkonten können die Optionen Heimatadresse und Standardadresse deaktiviert werden, obwohl nur eine E-Mail-Adresse zugeordnet ist.	29700
Bei der Synchronisation der Zuweisungen von SAP Gruppen, Rollen oder Profilen an SAP Benutzerkonten aus einem sekundären System werden die Zuweisungen nicht in der One Identity Manager-Datenbank gespeichert.	29848
Fehlerhafte Synchronisation von Objekten der Organisationsstruktur aus einem SAP HCM System (HROrgUnit).	30121
Beim Anlegen von SAP Benutzerkonten mit Parametern, E-Mail-Adressen, Telefon- oder Faxnummern wird der definierte Name der Zuweisungen (beispielsweise SAPComPhone.DistinguishedName) nicht gebildet.	30356
Bei Änderungen an SAP Benutzerkonten werden zu viele Nachberechnungsaufträge in die DBQueue eingestellt.	30361
Das Ereignis Insert wird für Einträge in der Tabelle HelperSAPUserInSAPRole nicht ausgelöst.	30367
Zuweisungen von SAP Rollen an SAP Benutzerkonten werden provisioniert, obwohl die zugeordneten Kategorien nicht übereinstimmen.	30386

Gelöstes Problem	Fehler ID
Bei mehreren Änderungen des zentralen Kennworts einer Person kurz nacheinander, beispielsweise durch den Password Capture Agent, wird nur die erste Änderung an die SAP Benutzerkonten übernommen.	30420
Die Firmenzuordnung von SAP Benutzerkonten wird nicht ins Zielsystem provisioniert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30453 bereitgestellt.	30453
Wenn ein bestehendes SAP Benutzerkonto den Automatisierungsgrad Full managed erhält, werden die IT Betriebsdaten für die SAP Kommunikationsdaten (SAPComPhone, SAPComFax und SAPComSMTP) nicht ermittelt.	30515
Fehler bei der Synchronisation von Firmendaten (Tabelle Company).	30557
Fehler beim Laden von Einzelobjekten für Schematypen, die über eine Schemaerweiterungsdatei bereitgestellt werden.	30653, 30701
Für ein SAP Benutzerkonto werden die ausführbaren SAP Transaktionen nicht korrekt ermittelt.	30718
Fehler bei der Berechnung von Rollenzuordnungen (Tabelle SAPUserInSAPRole).	30797, 31149
Fehler bei der Provisionierung, wenn im Manager die Option Produktivkennwort soll gesetzt werden für ein Benutzerkonto mit dem Benutzerkontentyp Service oder System gesetzt wurde.	30952, 30956
Fehlerhafte Bildungsregeln für die Spalten SAPComPhone.PhoneNumber und SAPComFax.FaxNumber.	31105
Fehler bei der Konvertierung von Json-Daten mit dem Datentyp Integer oder Float.	30536
Fehler beim Löschen von Gruppenmitgliedschaften mit dem SCIM Konnektor.	30710
Fehlerhafte Auflösung von Gruppenmitgliedschaften einer Cloud-Anwendung, wenn die Schemaeigenschaft members~type keinen Wert enthält.	31187
Die Konnektoren für Microsoft Exchange, Exchange Online und Windows PowerShell nutzen nur einen Revisionszähler, auch wenn mehrere Schemaeigenschaften je Schematyp als Revisionszähler gekennzeichnet sind. In Synchronisationsprojekten, die den Windows PowerShell Konnektor nutzen, muss das Zielsystemschemata neu geladen werden, um mehrere Revisionszähler nutzen zu können. In Synchronisationsprojekten für Microsoft Exchange und Exchange Online wird ein Patch mit der Patch ID VPR#31026 bereitgestellt.	31026
Beim Ermitteln der Manager für E-Mail-Benutzer und E-Mail-Kontakte in großen Exchange Online-Umgebung tritt eine Out-Of-Memory-Exception auf.	31087

Gelöstes Problem	Fehler ID
Der native Datenbankkonnektor löscht keine Gruppenmitgliedschaften im Zielsystem, wenn die Provisionierung durch einen Anwendungsserver ausgeführt wird.	30659
Bei der Synchronisation mit dem nativen Datenbankkonnektor werden Objekte als geändert gekennzeichnet, die nicht geändert wurden.	30840
Leerzeichen im Namen der Schemaeigenschaft, die als Revisionszähler gekennzeichnet ist, werden im nativen Datenbankkonnektor nicht maskiert.	30901

Tabelle 8: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Attestierungen werden mit der Begründung "es war kein Entscheider verfügbar" abgebrochen, obwohl ein Entscheider vorhanden ist.	30408
Die Customizermethode CreateAttestations blockiert unter Umständen die Abarbeitung der DBQueue.	31016
Fehler beim Löschen von Attestierungsläufen.	31092
Beim Deaktivieren von Attestierungsrichtlinien werden die zugehörigen Attestierungsvorgänge nicht gelöscht.	31141
In E-Mail-Benachrichtigungen an Attestierer fehlen die in der unternehmensspezifischen Mailvorlage definierten Bilder.	31151
Leistungspositionen können nicht als Produkte im IT Shop angelegt werden, wenn deren Bezeichnung länger als 128 Zeichen ist.	30399
Im Entscheidungsverlauf wird die Uhrzeit als UTC Zeit angezeigt.	30483
Das Skript VI_BuildITShopLink_Unsubscribe erzeugt einen fehlerhaften Link.	30531
Die Mitgliedschaft in einer Rolle kann nicht delegiert werden, wenn der Empfänger der Delegierung bereits direktes Mitglied dieser Rolle ist.	30549
Wenn eine Unternehmensressource gleichzeitig über eine befristete und eine unbefristete Bestellung zugewiesen wird und die befristete Bestellung abläuft, dann wird die Unternehmensressource entzogen, obwohl noch eine gültige, unbefristete Bestellung existiert.	30697
Die Bildungsregeln für die Spalten ShoppingCartItem.ObjectKeyAssignment, DisplayObjectKeyAssignment und PersonWantsOrg.DisplayObjectKeyAssignment sind nicht überschreibend.	30766
Beim Kopieren eines Entscheidungsworkflows friert der Manager ein.	30833
Beim Bestellen von Benutzerkonten im IT Shop werden die initialen Anmeldinformationen an die falsche Person versendet.	31014
Abgeschlossene Bestellungen werden nicht gelöscht, obwohl der Aufbe-	31068

Gelöstes Problem	Fehler ID
wahrungszeitraum abgelaufen sein müsste.	
Der DBQueue Prozessor überprüft automatische Entscheidungen auch für Bestellungen, die bereits genehmigt aber noch nicht zugewiesen sind (OrderState = 'Granted').	31076
Fehlerhafte Prüfung, ob eine Unternehmensressource bereits zugewiesen ist, wenn die Option Verwendung nur im IT Shop aktiviert wird.	31116
Wenn für ein Produkt mit einer Regelverletzung im Genehmigungsverfahren eine Ausnahme erteilt wurde, bleibt die Regelverletzung bestehen, nachdem das Produkt abbestellt und die Zuweisung entfernt wurde.	30213
Bei Ad-hoc-Regelprüfungen werden die Verarbeitungsaufträge zur Neuberechnung von Regelverletzungen und zur Berechnung der betroffenen Personengruppe nicht erzeugt. Dadurch werden die betroffenen Personen möglicherweise nicht korrekt ermittelt.	30281
Wenn eine deaktivierte Complianceregel gelöscht wird, werden die zugehörigen Regelverletzungen nicht gelöscht.	30585
Bei der Berechnung von Regelverletzungen werden auch deaktivierte Regeln berechnet.	30728
Fehler bei der Complianceberechnung nach einer Aktualisierung der One Identity Manager-Datenbank, bei der nur Module ausgewählt wurden, die keine Abhängigkeit zum Modul Complianceregeln haben.	30905
Falscher Tabellename im One Identity Manager Administrationshandbuch für Systemrollen, im Abschnitt Deaktivierte Systemrollen .	29226
Fehler beim Zuweisen eines Objekts aus einer kundenspezifischen Tabelle an eine Systemrolle.	30465
Seit Version 7.1.2 werden die Zuweisungen von Unternehmensressourcen an untergeordnete Systemrollen in der Tabelle EsetHasEntitlement nicht mehr abgebildet. Bei der Aktualisierung der One Identity Manager-Datenbank auf die Version 7.1.2 oder neuer werden bestehende Zuweisungen an untergeordnete Systemrollen jedoch nicht aus der Tabelle EsetHasEntitlement entfernt.	30614
Systembenutzer, denen sowohl die Rechtegruppe vi_4_PERSONADMIN als auch VI_4_ALLMANAGER zugewiesen ist, können keine Personen anlegen.	30052

Gelöstes Problem

Fehler ID

i HINWEIS: Durch die Lösung dieses Problems kann es nun passieren, dass Objekte nicht eingefügt werden können, da Spaltenrechte auf Pflichtfelder fehlen. Bei der Berechnung der einzelnen Spaltenrechte werden die Tabellenrechte der jeweiligen Rechtegruppe berücksichtigt. Die Tabellenrechte verschiedener Rechtegruppen werden nicht mehr auf alle Spalten übernommen. Damit kann eine Spalte beim Einfügen eines Objekts nicht bearbeitet werden, wenn für die Rechtegruppe, die das Spaltenrecht **Bearbeitbar** vergibt, kein Tabellenrecht **Einfügbar** definiert ist.

Im Manager wird die Aufgabe **Kennwortabfrage ändern** auch dann angezeigt, wenn der angemeldete Benutzer nicht die erforderlichen Berechtigungen dafür hat. 30287

Im Bericht **Herkunft von Berechtigungen anzeigen** fehlen SAP Rollen und BI Analyseberechtigungen, die über Systemrollen geerbt wurden. 30291

Fehler beim Anzeigen des Berichts **Berechtigungsüberblick einer Person zu einem definierten Zeitpunkt.** 30859

Darstellungsfehler im Filterdesigner 29639, 30668

- beim Erstellen von dynamischen Rollen mit vielen Filterkriterien
- wenn mehrere Elemente aus einer Auswahlliste ausgewählt werden

Beim Generieren von einfachen Berichten im CSV-Format wird ein leerer Bericht erzeugt. 31073

Siehe auch:

- [Schemaänderungen](#) auf Seite 49
- [Patches für Synchronisationsprojekte](#) auf Seite 58

Bekannte Probleme

Nachfolgend finden Sie eine Liste der zum Zeitpunkt der Freigabe dieser Version von One Identity Manager bekannten Probleme.

Tabelle 9: Allgemein

Bekanntes Problem	Fehler ID
Verbindet man sich mit dem Database Compiler gegen eine Datenbank, wird in die DBQueue sofort der Auftrag QBM-K-CommonWaitForCompiler eingestellt.	23049, 24713
Wird der Database Compiler beendet, ohne die Datenbank zu kompilieren, verbleibt der Auftrag in der DBQueue.	

Bekanntes Problem	Fehler ID
<p>Fehler im Report Editor, wenn im Bericht Spalten verwendet werden, die im Report Editor als Schlüsselworte definiert sind.</p> <p>Workaround: Erstellen Sie Datenabfragen als SQL-Abfragen und nutzen Sie für die betroffenen Spalten Aliasnamen.</p>	23521
<p>Wird der Web Installer gleichzeitig in mehreren Instanzen gestartet, kann es zu Zugriffsfehlern kommen.</p>	24198
<p>Header-Zeilen in als CSV gespeicherten Reporten enthalten keine sprechenden Namen.</p>	24657
<p>Nach einer Simulation im Manager sind Objekte unter Umständen im inkonsistenten Zustand. Wird ein Objekt während einer Simulation verändert, gespeichert und die Simulation beendet, so bleibt das Objekt im letzten Zustand der Simulation erhalten. Weitere Änderungen an dieser Objektinstanz können unter Umständen nicht gespeichert werden.</p> <p>Lösung: Laden Sie nach dem Beenden der Simulation das Objekt neu.</p>	12753
<p>Im Configuration Wizard können unzulässige Modulkombinationen ausgewählt werden. Dies führt erst bei Beginn der Schemainstallation zu Fehlern.</p> <p>Ursache: Der Configuration Wizard wurde direkt gestartet.</p> <p>Lösung: Verwenden Sie zur Installation der One Identity Manager Komponenten immer die autorun.exe. Damit ist sichergestellt, dass keine unzulässigen Modulkombinationen ausgewählt werden.</p>	25315
<p>Schemaerweiterungen an einer Datenbanksicht vom Typ View (beispielsweise Department) mit einer Fremdschlüsselbeziehung auf eine Spalte einer Basistabelle (beispielsweise BaseTree) oder einer Datenbanksicht vom Typ View sind nicht zulässig.</p>	27203
<p>Fehler bei der Verbindung über einen Anwendungsserver oder den API Server, wenn der private Schlüssel des Zertifikates, mit dem die VI.DB ihre Session-Information zu verschlüsseln versucht, nicht exportiert werden kann und der private Schlüssel damit der VI.DB nicht zur Verfügung steht.</p> <p>Lösung: Markieren Sie den privaten Schlüssel beim Export und Import des Zertifikats als exportierbar.</p>	27793
<p>Wenn eine One Identity Manager-Datenbank im Cluster betrieben wird, wird die Datenbank nach einem Clusterschwenk aus dem Backup wiederhergestellt. Dabei wird eine neue Datenbank-ID erzeugt. Dieser Schritt kann nicht mehr übersprungen werden, da die Datenbank sonst nicht kompiliert werden kann.</p>	28373
<p>Die kundenspezifische Erweiterung von vordefinierten dynamischen Fremdschlüsseln um Referenzen auf vordefinierte Tabellen ist nicht möglich. Wenn Sie kundenspezifische dynamische Fremdschlüssel definieren, muss mindes-</p>	29227

Bekanntes Problem	Fehler ID
<p>tens einer der beteiligten Partner - dynamische Fremdschlüsselspalte oder referenzierte Tabelle - ein kundenspezifisches Objekt sein.</p>	
<p>Fehler beim Auslösen von Ereignissen auf eine View , welche keine UID-Spalte als Primärschlüssel besitzt.</p> <p>Primärschlüssel für Objekte im One Identity Manager bestehen immer aus einer oder, bei M:N-Tabellen, zwei UID-Spalten. Dies ist eine Basisfunktionalität im System.</p> <p>Die Definition einer View, die als Primärschlüssel den XObjectKey verwendet, ist nicht zulässig und wird an sehr vielen Stellen zu weiteren Fehlern führen.</p> <p>Zur Überprüfung des Schemas wird eine Konsistenzprüfung Table of type U or R with wrong PK definition bereitgestellt.</p>	29535
<p>Die Standardeinstellungen der globallog.config gehen davon aus, dass die Rechte zum Schreiben in %localappdata% vorhanden sind. Hat eine EXE nicht die richtigen Berechtigungen, kann man durch Änderung der Variable logBaseDir in der globallog.config oder durch Einführung einer speziellen Log-Konfiguration in der *.exe.config oder web.config das Protokoll in ein Verzeichnis schreiben lassen, für das Rechte bestehen.</p>	30048
<p>Der One Identity Manager Service protokolliert Meldungen standardmäßig nur im Ereignisprotokoll Application.</p> <p>Ursache: Um ein Ereignisprotokoll mit einem anderen Namen anzulegen, werden administrative Berechtigungen auf dem Jobserver benötigt.</p> <p>Lösung:</p> <ol style="list-style-type: none"> 1. Legen Sie die Datei, in die der One Identity Manager Service schreiben soll, manuell auf dem Jobserver an. Nutzen Sie dafür beispielsweise Windows PowerShell. <ol style="list-style-type: none"> a. Führen Sie auf dem Jobserver Windows PowerShell als Administrator aus. b. Führen Sie folgendes CmdLet aus: <pre>New-EventLog -Source "Foobar" -LogName "<Dateiname>"</pre> 2. Geben Sie diesen Dateinamen in der Konfigurationsdatei des One Identity Manager Service, im Modul Logwriter als Namen für das Ereignisprotokoll an. 3. Starten Sie den Computer neu. 4. Starten Sie den One Identity Manager Service neu. 	30540
<p>Wenn die One Identity Manager-Datenbank in einem SQL-Cluster (High Availability Group) installiert ist und die Option DTC_SUPPORT = PER_DB gesetzt ist, erfolgt die Replikation zwischen den Servern mittels Distributed Transaction. Fehler, falls dabei ein Save Transaction ausgeführt wird: Cannot use SAVE</p>	30972

Bekanntes Problem	Fehler ID
<p>TRANSACTION within a distributed transaction.</p> <p>Lösung: Deaktivieren Sie die Option DTC_SUPPORT = PER_DB.</p>	

Tabelle 10: Webanwendungen

Bekanntes Problem	Fehler ID
<p>Bei der Installation des Web Portals mit dem Web Installer kann folgende Fehlermeldung auftreten: Diese Zugriffssteuerungsliste liegt nicht in der kanonischen Form vor und kann aus diesem Grund nicht geändert werden. Der Fehler tritt oft nach einem Windows 10 Anniversary Update auf.</p> <p>Lösung: Ändern Sie auf dem Elternordner der Webanwendung (standardmäßig C:\inetpub\wwwroot) die Berechtigungen für den Benutzer und wenden Sie diese Änderung an. Nehmen Sie anschließend diese Änderung wieder zurück.</p>	26739

Tabelle 11: Zielsystemanbindung

Bekanntes Problem	Fehler ID
<p>Bei Windows PowerShell Verbindungen, welche intern Import-PSSession verwenden, kommt es zu Speicherlecks.</p>	23795
<p>Nach der Synchronisation einer SAP R/3-Umgebung können die Zuweisungen von Einzelrollen an SAP Benutzerkonten als ausstehend gekennzeichnet sein. Das Problem kann auftreten, wenn</p> <ul style="list-style-type: none"> • die Zuweisungen von SAP Rollen an Benutzerkonten vor der Installation des One Identity Manager 7.0.1 in die One Identity Manager Datenbank eingelesen wurden und • die Zuweisungen von Einzelrollen, die Bestandteil von Sammelrollen sind, als direkte Zuweisungen abgebildet wurden. (Fehler ID 3218196) <p>Durch die Behebung dieses Fehlers im One Identity Manager 7.0.1 werden nach erneuter Synchronisation und bei entsprechender Synchronisationskonfiguration diese fehlerhaften Zuweisungen als ausstehend gekennzeichnet.</p> <p>Lösung: Löschen Sie die ausstehenden Zuweisungen im Zielsystemabgleich des One Identity Manager.</p>	
<p>Der Baustein HR_ENTRY_DATE eines SAP HCM Systems ist standardmäßig nicht remote aufrufbar.</p> <p>Lösung: Ermöglichen Sie den Remotezugriff auf den Baustein HR_ENTRY_DATE in Ihrem SAP HCM System. Erstellen Sie im Synchronization Editor das Mapping für die Schemaeigenschaft EntryDate.</p>	25401
<p>Beim Anlegen von Microsoft Exchange Postfächern werden gegebenenfalls</p>	27042

Bekanntes Problem	Fehler ID
<p>vorhandene sekundäre SIP-Adressen in primäre SIP-Adressen umgewandelt, sofern bisher keine primären SIP-Adressen hinterlegt waren.</p>	
<p>Der SAP Konnektor stellt keine Schemaeigenschaft bereit, um zu erkennen, ob ein Benutzer in der SAP R/3-Umgebung ein produktives Kennwort hat.</p> <p>Wenn diese Information im One Identity Manager zur Verfügung stehen soll, erweitern Sie das Schema und die Synchronisationskonfiguration.</p> <ul style="list-style-type: none"> • Legen Sie eine kundenspezifische Spalte an der Tabelle SAPUser an. • Erweitern Sie im Synchronisationsprojekt das SAP Schema um einen neuen Schematyp, der die benötigte Information liefert. • Passen Sie die Synchronisationskonfiguration an. 	27359
<p>Bei Verwendung der Bind-Methode Fast Bind in Active Directory können keine Kennwörter provisioniert werden. Die SetPassword-Methode ist somit nicht verfügbar.</p> <p>Der Prozessschritt AdhocProjection scheitert mit der Meldung:</p> <pre>[System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKONNNNAME)).</pre>	27427
<p>Synchronisationsprojekte für SAP R/3, die per Transport in eine One Identity Manager Datenbank importiert wurden, können nicht geöffnet werden. Das Problem tritt nur auf, wenn vor dem Import des Transportpakets noch kein SAP R/3 Synchronisationsprojekt in der Zieldatenbank angelegt wurde.</p> <p>Lösung: Erstellen und speichern Sie mindestens ein Synchronisationsprojekt für SAP R/3 in der Zieldatenbank, bevor Sie SAP R/3 Synchronisationsprojekte mit dem Database Transporter in diese Datenbank importieren.</p>	27687
<p>Fehler im IBM Notes Konnektor (Error getting revision of schema type ((Server))).</p> <p>Wahrscheinliche Ursache: Die IBM Notes-Umgebung wurde neu aufgebaut oder es wurden zahlreiche Einträge in das Domino-Verzeichnis eingefügt.</p> <p>Lösung: Aktualisieren Sie in der IBM Notes-Umgebung die Indexe im Domino-Verzeichnis manuell.</p>	27126
<p>Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer Zentralen Benutzerverwaltung.</p> <p>Meldung: No company is assigned.</p> <p>Ursache: Für das Benutzerkonto konnte keine Firmenadresse ermittelt werden.</p> <p>Lösung: Stellen Sie sicher, dass entweder</p> <ul style="list-style-type: none"> • jedem Benutzerkonto eine Firma zugeordnet ist, die im Zentralsystem 	29253

Bekanntes Problem	Fehler ID
<p>existiert</p> <p>- ODER -</p> <ul style="list-style-type: none"> dem Zentralsystem eine Firma zugeordnet ist. 	
<p>Fehler beim Laden von Einzelobjekten mit Windows PowerShell, wenn dabei der Parameter Identity genutzt wird. Der Fehler kann beispielsweise bei der Provisionierung von Objektänderungen in eine Microsoft Exchange-Umgebung oder eine Exchange Online-Umgebung auftreten und führt hier zu Folgefehlern.</p> <p>Meldung des Windows PowerShell Konnektors: Command yielded <Anzahl> objects but only one was expected.</p> <p>Ursache: Es sind mehrere gleichnamige Objekte vorhanden.</p>	29152
<p>Bei der Synchronisation von SAP R/3 Personalplanungsdaten, die erst zukünftig wirksam werden, werden einige Daten nicht eingelesen.</p> <p>Ursache: Die Funktion BAPI_EMPLOYEE_GETDATA wird immer mit dem aktuellen Tagesdatum ausgeführt. Damit werden Änderungen taggenau beachtet.</p> <p>Lösung: Für eine Vorab-Synchronisation von Personaldaten, die erst zukünftig wirksam werden, nutzen Sie eine Schemaerweiterung und lesen Sie die Daten aus der Tabelle PA0001 direkt ein.</p>	29556
<p>Fehler bei der Synchronisation einer OpenDJ-Umgebung, wenn ein Kennwort mit einer öffnenden geschweiften Klammer beginnt.</p> <p>Ursache: Der LDAP Server interpretiert ein generiertes Kennwort in der Form {<abc>}<def> als Hashwert. Der LDAP Server lässt die Übergabe von gehashten Kennwörtern jedoch nicht zu.</p> <p>Lösung: LDAP Server können so konfiguriert werden, dass ein bereits gehashtes Kennwort in der Form {<Algorithmus>}Hash übergeben wird.</p> <ul style="list-style-type: none"> Auf dem LDAP Server: Erlauben Sie die Übergabe von bereits gehashten Kennwörtern. Im Synchronisationsprojekt: Übergeben Sie nur gehashte Kennwörter. Nutzen Sie Skripteigenschaften für das Mapping von Schemaeigenschaften, die Kennwörter enthalten. Erzeugen Sie im Skript den Hashwert der Kennwörter. 	29620
<p>Der Zielsystemabgleich zeigt in der Manager Webanwendung keine Informationen an.</p> <p>Workaround: Nutzen Sie den Manager, um den Zielsystemabgleich durchzuführen.</p>	30271
<p>Bei Bestellung eines Zugriffs auf ein Asset aus dem Bereich einer Zugriffsanforderungsrichtlinie, die für assetbasierten Sitzungszugriff vom Typ Benutzer angegeben konfiguriert ist, tritt im One Identity Safeguard</p>	796028, 30963

Bekanntes Problem	Fehler ID
<p>folgender Fehler auf:</p> <p>400: Bad Request -- 60639: A valid account must be identified in the request.</p> <p>Die Bestellung wird im One Identity Manager abgelehnt und der Fehler in der Bestellung als Begründung angezeigt.</p>	
<p>Bei der Einrichtung eines Synchronisationsprojektes für One Identity Safeguard wird eine Fehlermeldung angezeigt:</p> <p>404: Not Found -- 0:</p> <p>Ursache: Es wird eine ältere One Identity Safeguard Version verwendet, die nicht von One Identity Manager unterstützt wird.</p> <p>Lösung: Stellen Sie sicher, dass die One Identity Safeguard Version 2.5 verwendet wird.</p>	31048
<p>Bei Inkonsistenzen in der SharePoint-Umgebung kann es passieren, dass bereits der Zugriff auf eine Eigenschaft einen Fehler verursacht. Der Fehler erscheint auch dann, wenn das Mapping der betroffenen Schemaeigenschaft deaktiviert wird.</p> <p>Ursache: Der SharePoint Konnektor lädt standardmäßig alle Objekteigenschaften in einen Cache.</p> <p>Lösung:</p> <ul style="list-style-type: none"> • Korrigieren Sie den Fehler im Zielsystem. <ul style="list-style-type: none"> - ODER - • Deaktivieren Sie den Cache in der Datei <ul style="list-style-type: none"> VI.Projector.SharePoint.<Version>.Host.exe.config. 	31017

Tabelle 12: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
<p>Unter SharePoint 2010 kann es zu einem Fehler bei der Synchronisation von SharePoint Websites kommen. Die Methode SPWeb.FirstUniqueRoleDefinitionWeb() löst eine ArgumentException aus. Weitere Informationen finden Sie unter https://support.microsoft.com/de-de/kb/2863929.</p>	24626
<p>Die Installation des One Identity Manager Service mit Server Installer auf einem Windows Server funktioniert nicht, wenn die Einstellung File and Printer Sharing am Server deaktiviert ist. Auf einem Domänen-Controller ist diese Einstellung aus Sicherheitsgründen deaktiviert.</p>	24784
<p>Beim Verbinden mit einer Oracle Database kommt es sporadisch zu einem der folgenden Fehler: TNS-12516, TNS-12519 oder ORA-12520. Erneute Verbindungsversuche sind jedoch meist erfolgreich.</p>	27830

Bekanntes Problem	Fehler ID
Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am Server konfigurierte Limit.	
In einem mehrseitigen Synchronisationsprotokoll kann nicht mit der Maus und mit den Pfeiltasten navigiert werden. Ursache: Die StimulReport.Net-Komponente der Firma Stimulsoft behandelt den Bericht als eine Seite.	29051
Gültiger CSS-Code verursacht einen Fehler unter Mono, wenn doppelte Schlüssel vorhanden sind. Weitere Informationen finden Sie unter https://github.com/mono/mono/issues/7455 .	762534, 762548, 29607
Mitgliedschaften in Active Directory Gruppen vom Typ Universal in einer untergeordneten Domäne werden im Zielsystem nicht entfernt, wenn eines der folgenden Windows Updates installiert ist: <ul style="list-style-type: none"> • Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 <p>Uns ist derzeit nicht bekannt, ob weitere Windows Updates zu diesem Fehler führen können.</p> <p>Der Active Directory Konnektor korrigiert dieses Fehlverhalten mit einem Workaround beim Aktualisieren der Mitgliederliste. Da dieser Workaround die Performance bei der Provisionierung von Active Directory Gruppen verschlechtern kann, wird er aus künftigen One Identity Manager Versionen wieder entfernt, sobald Microsoft diesen Fehler behoben hat.</p>	30575

Schemaänderungen

Nachfolgend finden Sie eine Übersicht der Schemaänderungen von One Identity Manager Version 8.0.2 zu Version 8.1.

Konfigurationsmodul

- Neue Spalte `DialogColumn.CanEditScript` für Skripte zum bedingten Entfernen des Bearbeitbarkeitsrechtes für Spalten.
- Neue Spalte `DialogColumn.CanSeeScript` für Skripte zum bedingten Entfernen des Sichtbarkeitsrechtes für Spalten.
- Neue Spalte `DialogColumn.IsElementProperty` um Spalten als Namensbestandteile für die Kennwortprüfung zu kennzeichnen.
- Neue Spalte `DialogConfigParm.UID_QBMC1rTypeEditor` um einen Editor für die Bearbeitung komplexer Konfigurationsparameter anzubinden.

- Neue Spalte `DialogDatabase.LicenceID` als Kennzeichen für Lizenzinformationen.
- Neue Spalte `DialogDatabase.ProductionLevelAddOn` (in Vorbereitung).
- Neue Spalte `DialogAEDSAction.IsInActive` um einzelne Objekte zu deaktivieren.
- Neue Spalten `DialogReportQuery.HAssignFKColumn`, `DialogReportQuery.HAssignType`, `DialogReportQuery.HListColumns` und `DialogReportQuery.HObjColumns` für Abfragen für Berichte mit historischen Daten.
- Neue Spalte `DialogTag.SortOrder` als Sortierungsreihenfolge für Änderungskennzeichen.
- Neue Spalten `DialogTree.ListActivationFKList` und `DialogTree.NodeActivationFKList` zur Navigation zum Fremdschlüsselobjekt, das bei der Auswahl eines Eintrags in der Benutzeroberfläche geladen werden sollen.
- Neue Spalte `DialogUser.IsLockedOut` zur Angabe, ob ein Benutzer aufgrund fehlerhafter Anmeldeversuche gesperrt ist.
- Neue Spalte `DialogValidDynamicRef.IsForAddElementAffected` und `QBMRRelation.IsForAddElementAffected` zur Kennzeichnung, ob das übergeordnete Objekt in die Jobqueue übernommen werden soll.
- Neue Spalten `Job.IsNoDBQueueDefer`, `JobQueue.IsNoDBQueueDefer` und `JobTask.IsNoDBQueueDefer` als Kennzeichen, ob bei der Prozessverarbeitung auf die Verarbeitung von DBQueue Prozessor Aufträgen gewartet werden soll.
- Neue Spalte `QBMDBQueueSlot.XObjectKey`.
- Neue Spalte `QBMSJobqueueOverview.IsInitQueueRunning` als Kennzeichen, ob die Jobqueue initialisiert wird.
- Neue Spalten `QBMPwdPolicy.IsLowerLetterNotAllowed`, `QBMPwdPolicy.IsNumberNotAllowed`, `QBMPwdPolicy.IsSpecialNotAllowed` und `QBMPwdPolicy.IsUpperLetterNotAllowed` für Kennwortrichtlinien.
- Neue Spalte `QBMServer.LastJobFetchTime` als Zeitpunkt des letzten Prozessabrufs.
- Neue Spalte `QBMServer.PortNumber` als Port zur Anzeige der One Identity Manager Service Protokolldatei über einen Browser.
- Neue Spalten `QBMSVSystemOverview.QualityOfValue` und `QBMSVSystemOverview.RecommendedValue` zur Anzeige im Bericht über die Systemkonfiguration.
- Neue Spalte `QBMSWebApplication.UID_QBMSIdentityClient` zur Zuordnung einer OAuth 2.0/OpenID Connect Konfiguration zu Webanwendungen.
- Neue Tabelle `DialogGroupHasAEDS` zur Abbildung von Berechtigungen für API-Dateien.
- Neue Tabelle `DialogGroupInProductLimited` zur Zuweisung von Rechtegruppen an Anwendungen.
- Neue Tabelle `DialogObjectHasMethod` zur Zuweisung von Methodendefinitionen an Objektdefinitionen.
- Neue Tabellen `QBMDBPrincipal`, `QBMDBRoleDef`, `QBMDBPrincipalHasRoleDef` und `QBMDBRightsAddOn` zur Abbildung abgestufter Berechtigungen auf SQL Server- und

Datenbankebene.

- Neue Tabelle `QBMDBQueueTaskPerf` zur Auswertung der DBQueue Prozessor Auftragsperformance.
- Neue Tabellen `QBMDevBranch` und `QBMDevBranchHasAssembly` für die Versionsverwaltung von API-Projekten.
- Neue Tabelle `QBHTMLApp` für die Abbildung von Informationen zu HTML-Anwendungen.
- Neue Tabellen `QBMIIdentityClient`, `QBMIIdentityProvider`, `QBMIIdentityProvDisabledCol` und `QBMIIdentityProvEnabledCol` zur OAuth 2.0/OpenID Connect Konfiguration.
- Neue Tabelle `QBMLaunchActionHasFeature` zur Berechtigung von Launchpad Aktionen über Programmfunktionen.
- Neue Tabelle `QBMRReportQueryCriteria` zur Definition mehrerer Kriterien für historische Berichte.
- Neue Tabelle `QBMVNonUniqueMAllTable` zur Auflistung der Tabellen, bei denen die Kombination aus Objektschlüssel und Fremdschlüssel nicht Unique ist (zur Optimierung der Indexgenerierung).
- Folgende Tabellen wurden gelöscht:
 - `DialogValidParent`
 - `QBMPermissionSettingBase`
- Folgende Spalten wurden gelöscht:
 - `DialogDatabase.IsFullTextEnabled`
 - `DialogMethod.UID_DialogObject`
 - `DialogReportQuery.HListCriteriaColumn`
 - `DialogReportQuery.HListCriteriaValue`
 - `QBWebApplication.CertificateEndpoint`
 - `QBWebApplication.CertificateText`
 - `QBWebApplication.OAuthCertificateSubject`
 - `QBWebApplication.OAuthCertificateThumbPrint`
 - `QBWebApplication.OAuthResource`
 - `QBWebApplication.SharedSecret`

Modul Zielsystemsynchronisation

- Neue Spalte `DPRNameSpaceHasDialogTable.RootObjectPath` als Pfad zum Basisobjekt.
- Neue Spalte `DPRProjectionConfig.LogVariableSetContents` als Kennzeichen, ob Variablensets mit den aktuellen Werten protokolliert werden.
- Neue Spalten `DPRProjectionConfigStep.CommitPropertiesLeft`, `DPRProjectionConfigStep.CommitPropertiesMode` und `DPRProjectionConfigStep.CommitPropertiesRight` zur Verbesserung der objektbasierten Synchronisation.

- Neue Spalte `DPRSchemaMethod.MethodType` zur Kennzeichnung von Verarbeitungsmethoden.
- Neue Spalten `DPRShell.EditedBy` und `DPRShell.EditedSince` zur Kennzeichnung, ob ein Synchronisationsprojekt bereits in Bearbeitung ist.
- Neue Spalten `DPRShell.ShadowCopy` und `DPRShell.ShadowCopyMode` zur Optimierung des Ladeverhaltens von Synchronisationsprojekten.
- Neue Spalte `DPRSystemConnection.DisplayNameQualified` als vollständiger Anzeigename für die Systemverbindung.
- Neue Spalte `DPRTemplate.SortOrder` zur Sortierung von Projektvorlagen.
- Neue Tabelle `DPRScript` als Skriptbibliothek.
- Neue Tabellen `DPRStartSequence` und `DPRStartSequenceHasProjection` zum Verwalten von Startfolgen.

Zielsystem Basismodul

- Neue Pflichtfelddefinition für folgende Spalten:
 - `TSBAccountDef.ObjectKeyTargetSystem`
 - `TSBITData.ObjectKeyAppliesTo`
- Die Tabelle `TSBVGroupTable` wurde gelöscht.
- Die Spalte `UNSRoot.isMemberOfEnabled` wurde gelöscht.

Active Directory Modul

- Neue Spalte `ADSAccount.MSDsConsistencyGuid` als Referenz zum Cloud Benutzerkonto.
- Neue Spalte `ADSSite.UID_ADSEForest` als Verweis auf die Gesamtstruktur.
- Neue Pflichtfelddefinition für folgende Spalten:
 - `ADSContainer.UID_ADSDomain`
 - `ADSPolicy.UID_ADSDomain`
 - `ADSPrinter.UID_ADSMachine`
 - `ADSDomain.UID_ADSEForest`
- Die Spalte `ADSSite.UID_ADSDomain` wurde gelöscht.

Microsoft Exchange Modul

- Neue Spalte `EX0RoleAssignPolicy.XMarkedForDeletion` zur Kennzeichnung, ob eine Richtlinie zum Löschen markiert ist.
- Neue Pflichtfelddefinition für folgende Spalten:
 - `EX0ActiveSyncMBPolicy.UID_EX0Organization`
 - `EX0AddrList.UID_EX0Organization`
 - `EX0DAG.UID_EX0Organization`

EX0DL.UID_EX0Organization
EX0DynDL.UID_EX0Organization
EX0MailBox.UID_EX0Organization
EX0MailBoxDatabase.UID_EX0Organization
EX0MailContact.UID_EX0Organization
EX0MailPublicFolder.UID_EX0Organization
EX0MailUser.UID_EX0Organization
EX0ManagedFolderPolicy.UID_EX0Organization
EX0OfflAddrBook.UID_EX0Organization
EX0PublicFolder.UID_EX0Organization
EX0PublicFolderDatabase.UID_EX0Organization
EX0RetentionPolicy.UID_EX0Organization
EX0RoleAssignPolicy.UID_EX0Organization
EX0Server.UID_EX0Organization

Exchange Hybrid Modul

- Neue Spalte EXHRemoteMailbox.EmailAddresses zur Abbildung weiterer E-Mail-Adressen für Remotepostfächer.
- Neue Spalte EXHRemoteMailbox.EmailAddressPolicyEnabled zur Angabe, ob die E-Mail-Adresse anhand der Empfängerrichtlinien automatisch aktualisiert werden soll.
- Neue Pflichtfelddefinition für die Spalte EXHRemoteMailbox.UID_EX0Organization.

IBM Notes Modul

- Neue Pflichtfelddefinition für folgende Spalten:

NDOAdmin4.UID_NDODomain
NDOCertifier.UID_NDODomain
NDOCertifierRequest.UID_NDODomain
NDODGroup.UID_NDODomain
NDOMailInDB.UID_NDODomain
NDOServer.UID_NDODomain
NDODUser.UID_NDODomain

LDAP Modul

- Neue Pflichtfelddefinition für die Spalte LDAPContainer.UID_LDPDomain.

Oracle E-Business Suite Modul

- Neue Pflichtfelddefinition für folgende Spalten:

EBSApplication.UID_EBSSystem
EBSDataGroup.UID_EBSSystem
EBSMenu.UID_EBSSystem
EBSResp.UID_EBSSystem
EBSSecurityGroup.UID_EBSSystem
EBSUser.UID_EBSSystem

SharePoint Modul

- Neue Spalten SPSGroupPermission.XMarkedForDeletion und SPSUserPermission.XMarkedForDeletion zur Kennzeichnung, ob die Berechtigungen zum Löschen markiert sind.

- Neue Pflichtfelddefinition für folgende Spalten:

SPSLanguage.UID_SPSFarm
SPSWebApplication.UID_SPSFarm
SPSSite.UID_SPSWebApplication

SAP R/3 Benutzermanagement-Modul

- Neue Spalte SAPUserHasParameter.ParameterValueDirect zur Ermittlung der direkt im Zielsystem zugewiesenen Parameterwerte.
- Neue Spalte SAPUserInSAPRole.DisplayValue als Anzeigename für Mitgliedschaften.
- Neue Tabellen SAPBaseTreeHasParameter, DepartmentHasSAPPParameter, LocalityHasSAPPParameter, OrgHasSAPPParameter und ProfitCenterHasSAPPParameter zur Zuweisung von SAP Parametern an Unternehmensstrukturen.
- Neue Tabelle SAPUserMandant zur Abbildung von Zugriffsberechtigungen in ZBV-Systemen.

- Neue Pflichtfelddefinition für folgende Spalten:

SAPProfitCenter.UID_SAPMandant
SAPMandant.UID_SAPSystem
SAPLoginLanguages.UID_SAPSystem

- Die Tabelle SAPUserInSAPMandant wurde gelöscht.

Modul SAP R/3 Compliance Add-on

- Neue Spalte XMarkedForDeletion an den Tabellen SAPAuthObjectClass, SAPBaseTreeInSAPFunction, SAPFieldHasSAPRCTable, SAPFunctionInstanceDetail, SAPRCTable, SAPRCVariable, SAPTransactionHasSAPAuthObject und SAPUserInSAPFunction

zur Kennzeichnung, ob die Objekte zum Löschen markiert sind.

- Neue Pflichtfelddefinition für folgende Spalten:

`SAPAuthObject.UID_SAPSystem`

`SAPAuthObjectClass.UID_SAPSystem`

`SAPVariableSet.UID_SAPMandant`

Privileged Account Governance Modul

- Neues Datenmodell für das Privileged Account Governance Modul.

Identity Management Basismodul

- Neue Spalten `AERole.UID_PersonHead` und `AERole.UID_PersonHeadSecond` zur Abbildung von Verantwortlichen für Anwendungsrollen.
- Neue Spalte `Person.ContactEmail` als Kontakt-E-Mail-Adresse für das Selbstregistrierungsportal.
- Neue Spalte `Person.EmployeeType` zur Abbildung von Mitarbeitertypen.
- Neue Spalte `Person.IsLockedOut` zur Angabe, ob die Person aufgrund fehlerhafter Anmeldeversuche gesperrt ist.
- Neue Spalte `Person.IsLockedPwdAnswer` zur Angabe, ob der Dialog zum Ändern des Kennwortes aufgrund fehlerhafter Antworten gesperrt ist.
- Neue Spalte `Person.UID_DialogCultureFormat` zur Angabe einer Sprache für die sprachspezifische Anzeige von Zahlen und Datumsangaben in der Benutzeroberfläche des Web Portals.
- Neue Spalten `PersonWantsOrg.CheckResult`, `PersonWantsOrg.CheckResultDetail`, `ShoppingCartItem.CheckResult`, `ShoppingCartItem.CheckResultDetail` und `ShoppingCartOrder.CheckStatus` für die asynchrone Verarbeitung von Bestellungen.
- Neue Spalten `PWODecisionMethod.UID_DialogRichMailProlongate` und `PWODecisionMethod.UID_DialogRichMailUnsubscribe` zur Angabe weiterer Mailvorlagen an Entscheidungsrichtlinien.
- Neue Spalte `QERJustification.JustificationType` zur Angabe eines Nutzungstyps von Standardbegründungen.
- Neue Tabelle `BaseTreeOwnsObject` für die schnellere Ermittlung von Zielsystemverantwortlichen.
- Neue Tabelle `QEROrgRootHasOrgType` zur Festlegung von Rollentypen für Rollenklassen.
- Neue Tabelle `QERPasswordQueryAndAnswer` für Kennwortfragen und -antworten für die Kennwortrücksetzung.
- Neue Tabelle `QERVPersonCentralPwdColumn` zur Festlegung der Benutzerkontoeigenschaften, auf die das zentrale Kennwort von Personen abgebildet werden soll.
- Verlängerung folgender Spalten von `nvarchar(128)` auf `nvarchar(256)`:
 - `AERole.Ident_AERole`

BaseTree.Ident_Org
DelegableItem.DisplayValue
QERVDelegableItem.DisplayValue
Department.DepartmentName
ITShopOrg.Ident_Org
ITShopSrc.Ident_Org
Locality.Ident_Locality
PersonWantsOrg.DisplayOrg
PersonWantsOrg.DisplayOrgParent
PersonWantsOrg.DisplayOrgParentOfParent
ProfitCenter.ShortName
ShoppingCartItem.DisplayOrg

- Folgende Spalten wurden gelöscht:

Person.PasswordAnswer
Person.PasswordQuery

Geschäftsrollenmodul

- Verlängerung der Spalte Org.Ident_Org von nvarchar(128) auf nvarchar(256).

Modul Attestierung

- Neue Spalte AttestationHelper.UID_PWORulerOrigin zur Ermittlung der Attestierer.

Modul Complianceregeln

- Verlängerung der Spalte NonCompliance.Ident_NonCompliance von nvarchar(128) auf nvarchar(256).

Helpdeskmodul

- Neue Spalte HDSSupporterGroup.XMarkedForDeletion zur Kennzeichnung, ob eine Bearbeitergruppe zum Löschen markiert ist.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 8.0.2 zu Version 8.1. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 79.

Änderungen an Synchronisationsvorlagen

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen. Um Änderungen an Synchronisationsvorlagen in bestehende Synchronisationsprojekte zu übernehmen, werden Patches bereitgestellt. Weitere Informationen finden Sie unter [Patches für Synchronisationsprojekte](#) auf Seite 58.

Tabelle 13: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Azure Active Directory Modul	Azure Active Directory Synchronization	keine
Active Directory Modul	Active Directory Synchronization	geändert
Active Roles Modul	Synchronize Active Directory Domain via Active Roles	geändert
Modul Cloud Systems Management	Universal Cloud Interface synchronization	keine
Oracle E-Business Suite Modul	Oracle E-Business Suite Synchronization	geändert
	Oracle E-Business Suite CRM data	geändert
	Oracle E-Business Suite HR data	geändert
	Oracle E-Business Suite OIM data	geändert
Microsoft Exchange Modul	Microsoft Exchange 2010 Synchronization (abgekündigt)	keine
	Microsoft Exchange 2013 / 2016 Synchronization (abgekündigt)	keine
	Microsoft Exchange 2010 Synchronization (v2)	geändert
	Microsoft Exchange 2013_2016 Synchronization (v2)	geändert
G Suite Modul	G Suite Synchronization	geändert
LDAP Modul	AD LDS Synchronization	keine
	OpenDJ Synchronization	keine
IBM Notes Modul	Lotus Domino synchronization	geändert
Exchange Online Modul	Exchange Online Synchronization (abgekündigt)	geändert
	Exchange Online Synchronization (v2)	geändert
Privileged Account Gover-	One Identity Safeguard Synchronization	neu

Modul	Synchronisationsvorlage	Art der Änderung
nance Modul		
SAP R/3 Benutzermanagement-Modul	SAP R/3 Synchronization (Base Administration)	geändert
	SAP R/3 (CUA subsystem)	keine
Modul SAP R/3 Analyseberechtigungen Add-on	SAP R/3 BW	keine
Modul SAP R/3 Compliance Add-on	SAP R/3 authorization objects	keine
Modul SAP R/3 Strukturelle Profile Add-on	SAP R/3 HCM authentication objects	keine
	SAP R/3 HCM employee objects	keine
SharePoint Modul	SharePoint Synchronization	keine
SharePoint Online Modul	SharePoint Online Synchronization	keine
Modul Universal Cloud Interface	SCIM Connect via One Identity Starling Connect	geändert
	SCIM Synchronization	geändert
Modul Unix-basierte Zielsysteme	Unix Account Management	keine
	AIX Account Management	keine

Patches für Synchronisationsprojekte

Im One Identity Manager 8.1 werden Patches für folgende Patchtypen bereitgestellt:

- Patches für gelöste Probleme
- Patches für neue Funktionen
- Meilensteine

Um bestehende Synchronisationsprojekte an die One Identity Manager Version 8.1 anzupassen, müssen die Meilensteine angewendet werden. Je Kontext wird ein Meilenstein bereitgestellt. Ein Meilenstein fasst alle Patches für gelöste Probleme und die Meilensteine der Vorversionen zusammen, wenn diese noch nicht angewendet wurden. Sobald der aktuelle Meilenstein auf ein Synchronisationsprojekt angewendet wurde, ist dieses Synchronisationsprojekt mit dem One Identity Manager 8.1 kompatibel.

Patches für neue Funktionen können optional angewendet werden.

Nachfolgend finden Sie eine Liste der Patches für Synchronisationsprojekte, die im One Identity Manager 8.1 neu bereitgestellt werden. Es sind nur die Patches aufgelistet, die

nach der Version 8.0.2 neu erstellt wurden. Einen Überblick über die Patches früherer One Identity Manager Versionen erhalten Sie in den jeweiligen Versionsinformationen für diese Versionen.

Jeder Patch enthält ein Skript, welches prüft, ob der Patch auf das Synchronisationsprojekt angewendet werden kann. Ob ein Patch angewendet werden kann, ist abhängig von der konkreten Synchronisationskonfiguration.

TIPP: Wenden Sie zuerst die Meilensteine an und danach die optionalen Patches für neue Funktionen.

Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 79.

Tabelle 14: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext DPR .	
	Meilenstein 8.1	Meilenstein für den Kontext One Identity Manager .	

Tabelle 15: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext Azure Active Directory .	

Tabelle 16: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#29087	Hinzufügen der Schemaeigenschaft mS-DS-ConsistencyGuid	Fügt die Schemaeigenschaft mS-DS-ConsistencyGuid in die Mappings User und InetOrgPerson ein.	29087
VPR#29306	Korrektur der Schema-klasse ADSSite (all) (Teil 1)	Ändert den Fremdschlüssel für ADSSite von ADSDomain zu ADSForest. Voraussetzung für Patch Korrektur der Schemaklasse ADSSite (all) (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	29306
VPR#29306_2	Korrektur der Schema-klasse ADSSite (all) (Teil 2)	Ändert den Fremdschlüssel für ADSSite von ADSDomain zu ADSForest. Abhängig von Patch Korrektur der	29306

Patch ID	Patch	Beschreibung	Fehler ID
		Schemaklasse ADSSite (all) (Teil 1). Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
VPR#30192	Definition eines Scopes und Nutzung der Verarbeitungsmethode MarkAsOutstanding	Fügt einen Scope hinzu und die Verarbeitungsmethode MarkAsOutstanding in den Synchronisationsschritt trustedDomain ein.	30192
	Meilenstein 8.1	Meilenstein für den Kontext Active Directory .	

Tabelle 17: Patches für Active Roles

Patch ID	Patch	Beschreibung	Fehler ID
VPR#28612	Neue Property-Mapping-Regeln im Mapping Computer	Fügt Property-Mapping-Regeln für OperatingSystem, OperatingSystemVersion und OperatingSystemServicePack in das Mapping Computer ein.	28612
VPR#29087	Hinzufügen der Schemaeigenschaft mS-DS-ConsistencyGuid	Fügt die Schemaeigenschaft mS-DS-ConsistencyGuid in die Mappings User und InetOrgPerson ein.	29087
	Meilenstein 8.1	Meilenstein für den Kontext Active Roles .	

Tabelle 18: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#28962_ EBS	Datumskonvertierung in Skripteigenschaften ändern	Bei der Konvertierung von Datumswerten in Skripteigenschaften wird ein kulturunabhängiges Format genutzt. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	28962
VPR#29265	Ergänzen einer Verarbeitungsmethode im Synchronisationsschritt HR PersonManager	Ergänzt die Verarbeitungsmethode EBS_Person_RemoveManager im Synchronisationsschritt HR	29265

Patch ID	Patch	Beschreibung	Fehler ID
		<p>PersonManager.</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	
VPR#29741	Erweiterung der Synchronisationskonfiguration um HR PersonPrimaryLocation	Ergänzt einen Synchronisationsschritt und ein Mapping für die Synchronisation des primären Standorts von Personen.	29741
VPR#30464	Unterstützung von Oracle Database Editionen	Fügt eine Variable zur Konfiguration der Oracle Database Edition ein.	30464
VPR#31011	Ändert das Serialisierungsformat	<p>Ändert das Serialisierungsformat an den Schematypen. Das Zielsystemschemata wird neu geladen.</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	31011
	Meilenstein 8.1	Meilenstein für den Kontext Oracle E-Business Suite.	

Tabelle 19: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#28815	Ergänzen einer Verarbeitungsmethode im Synchronisationsschritt RoleAssignmentPolicy	Ergänzt die Verarbeitungsmethode MarkAsOutstanding im Synchronisationsschritt RoleAssignmentPolicy.	28815
VPR#31026	Optimierung der Revisionsfilterung	Lädt das Zielsystemschemata neu und ersetzt die Revisionszähler whenChangedUTC und whenCreatedUTC durch vrtRevision.	31026
	Meilenstein 8.1	Meilenstein für den Kontext Microsoft Exchange.	

Tabelle 20: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30498	Entfernen von Property-Mapping-Regeln aus dem Mapping OwaMailboxPolicy	Entfernt die Property-Mapping-Regeln BoxAttachmentsEnabled, DropboxAttachmentsEnabled und GoogleDriveAttachmentsEnabled aus dem Mapping OwaMailboxPolicy.	30498
VPR#30588	Erweitern von Schemaeigenschaften und Property-Mapping-Regeln in den Mappings Calendar Processing (User/Shared) und Calendar Processing (Resource)	Erweitert die Mitgliederlisten in den Schemaeigenschaften vrtBookInPolicy, vrtRequestInPolicy und vrtRequestOutOfPolicy und passt die Property-Mapping-Regeln entsprechend an.	30588
VPR#31026	Optimierung der Revisionsfilterung	Lädt das Zielsystemschemata neu und ersetzt die Revisionszähler whenChangedUTC und whenCreatedUTC durch vrtRevision.	31026
VPR#31269	Erweiterung verschiedener Property-Mapping-Regeln um eine Bedingung für die Anwendung.	Ergänzt in verschiedenen Property-Mapping-Regeln im Mailbox-Mapping eine Bedingung für die Anwendung.	31269
	Meilenstein 8.1	Meilenstein für den Kontext Exchange Online .	

Tabelle 21: Patches für G Suite

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext G Suite .	

Tabelle 22: Patches für LDAP

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext LDAP .	

Tabelle 23: Patches für IBM Notes

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30313	Mapping von Zugriffsstufen für Postfachdateien	Fügt eine Property-Mapping-Regel für die Zugriffsstufen von Postfachdateien in das Mapping Person ein.	30313
	Meilenstein 8.1	Meilenstein für den Kontext IBM Notes .	

Tabelle 24: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#28147	Löscht das Mapping userInMandant	Löscht das Mapping userInMandant. Das Mapping wird ersetzt durch userMandant. Voraussetzung für Patch Neues Mapping userMandant . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	28147
VPR#28147_2	Neues Mapping userMandant	Neues Mapping für den Zugriff von Benutzerkonten auf Mandanten (userMandant). Abhängig von Patch Löscht das Mapping userInMandant . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	28147
VPR#30453	Neue Property-Mapping-Regel für die Provisionierung von Firmendaten.	Neue Property-Mapping-Regel am Mapping der Benutzerkonten für die Provisionierung von Firmendaten. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	30453
VPR#30941	Definiert auszuschließende Regeln für die Provisionierung	Definiert auszuschließende Property-Mapping-Regeln im Synchronisationsschritt userInCUARole des Provisionierungsworkflows. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	30941
	Meilenstein 8.1	Meilenstein für den Kontext SAP R/3 .	

Tabelle 25: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

Patch ID	Patch	Beschreibung	Fehler ID
VPR#29265	Ergänzen einer Verarbeitungsmethode im Synchronisationsschritt Managers	Ergänzt die Verarbeitungsmethode SHR_Department_RemoveManager im Synchronisationsschritt Managers. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	29265

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext SAP R/3 Strukturelle Profile Add-on .	

Tabelle 26: Patches für SAP R/3 BI Analyseberechtigungen

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext SAP R/3 Analyseberechtigungen Add-on .	

Tabelle 27: Patches für SAP R/3 Berechtigungsobjekte

Patch ID	Patch	Beschreibung	Fehler ID
VPR#29477	Anwenden der Verarbeitungsmethode MarkAsOutstanding	Wendet die Verarbeitungsmethode MarkAsOutstanding in verschiedenen Synchronisationsschritten an.	29477
	Meilenstein 8.1	Meilenstein für den Kontext SAP R/3 .	

Tabelle 28: Patches für SharePoint

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext SharePoint .	

Tabelle 29: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30729	Korrigieren der Eigenschaft Pflichtfeld des SharePoint Online User.LoginName	Korrigiert die Eigenschaft Pflichtfeld der Schemaeigenschaft LoginName in der Schemaklasse User (alle). Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	30729
	Meilenstein 8.1	Meilenstein für den Kontext SharePoint Online .	

Tabelle 30: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30497	Ermöglicht die Konfiguration des	Fügt eine Variable hinzu, über welche die Nutzung des lokalen Caches deaktiviert	30497

Patch ID	Patch	Beschreibung	Fehler ID
	lokalen Caches	werden kann. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 8.1	Meilenstein für den Kontext SCIM .	

Tabelle 31: Patches für die Universal Cloud Interface-Schnittstelle (im Modul Cloud Systems Management)

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext Universal Cloud Interface .	

Tabelle 32: Patches für Unix

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext Unix .	

Tabelle 33: Patches für den One Identity Manager Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext Datenbank .	

Tabelle 34: Patches für den CSV-Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1	Meilenstein für den Kontext CSV .	

Abgekündigte Funktionen

Mit dieser One Identity Manager Version werden folgende Funktionen nicht mehr unterstützt:

- Oracle Database als Datenbanksystem für die One Identity Manager-Datenbank wird nicht mehr unterstützt.

HINWEIS: Um die Umstellung des Datenbanksystems zu unterstützen, steht das Werkzeug Oracle Data Migrator zur Verfügung. Der Oracle Data Migrator übernimmt alle Daten eines Oracle Database Datenbankbenutzers der Version 8.0.1, oder eines neueren Service Packs, in eine SQL Server Datenbank mit derselben Version.

Das Werkzeug und eine Kurzanleitung werden über den Support zur Verfügung gestellt. Das Support Portal ist unter <https://support.oneidentity.com/identity-manager/> erreichbar.

- Die Prozesskomponente SvnComponent wurde entfernt.
- Google ReCAPTCHA Version 1 wird nicht mehr unterstützt.

Folgende Funktionen werden für künftige One Identity Manager Versionen abgekündigt und sollten nicht mehr verwendet werden:

- Die Nachbarschaftshilfe sowie Kennwortfragen und -antworten werden im Manager zukünftig nicht mehr unterstützt.

Verwenden Sie das Kennworrücksetzungsportal um Kennwörter zu ändern. Kennwortfragen und -antworten hinterlegen Sie im Web Portal.

- Der Konfigurationsparameter **QER | Person | UseCentralPassword | PermanentStore** wird zukünftig nicht mehr unterstützt und gelöscht.
- Die Tabelle OS wird zukünftig nicht mehr unterstützt und aus dem One Identity Manager Schema entfernt.

Systemanforderungen

Stellen Sie vor der Installation von One Identity Manager sicher, dass Ihr System den nachfolgenden minimalen Hardware- und Systemanforderungen genügt. Für detaillierte Informationen zu den Systemvoraussetzungen lesen Sie das *One Identity Manager Installationshandbuch*.

Minimalanforderungen für Datenbankserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
	HINWEIS: Aus Performancegründen wird der Einsatz von 16 physischen Kernen empfohlen.
Arbeitsspeicher	16 GB+ RAM
Freier Festplattenspeicher	100 GB

Betriebssystem	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. <p>UNIX und Linux Betriebssysteme</p> <ul style="list-style-type: none"> • Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.
Software	<p>Unterstützt werden die Versionen:</p> <ul style="list-style-type: none"> • SQL Server 2017 Standard Edition (64-Bit) mit aktuellem kumulativen Update • SQL Server 2016 Standard Edition (64-Bit), Service Pack 2 mit aktuellem kumulativen Update • Kompatibilitätsgrad für Datenbanken: SQL Server 2016 (130) • Standard-Sortierschema: Case-Insensitiv, SQL_Latin1_General_CP1_CI_AS (Empfehlung) <p>HINWEIS: Aus Performancegründen wird dringend der Einsatz der SQL Server Enterprise Edition empfohlen.</p>

Minimalanforderungen für Dienstserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	16 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	<p>Windows Betriebssysteme</p> <p>Unterstützt werden die Versionen:</p> <ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1 <p>Linux Betriebssysteme</p> <ul style="list-style-type: none"> • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden.

Zusätzliche Software	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Microsoft .NET Framework Version 4.7.2 oder höher <p>i HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers.</p> <p>Linux Betriebssysteme</p> <ul style="list-style-type: none"> • Mono 5.14 oder höher
----------------------	---

Minimalanforderungen für Clients

Prozessor	4 physische Kerne mit 2 GHz+ Taktung
Arbeitsspeicher	4 GB+ RAM
Freier Festplattenspeicher	1 GB
Betriebssystem	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Windows 10 (32-Bit oder 64-Bit) mindestens Version 1511 • Windows 8.1 (32-Bit oder 64-Bit) mit dem aktuellen Service Pack • Windows 7 (32-Bit oder nicht-Itanium 64-Bit) mit dem aktuellen Service Pack
Zusätzliche Software	<ul style="list-style-type: none"> • Microsoft .NET Framework Version 4.7.2 oder höher
Unterstützte Browserversionen	<ul style="list-style-type: none"> • Internet Explorer 11 oder höher • Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimalanforderungen für Webserver

Prozessor	4 physische Kerne mit 1.65 GHz+Taktung
Arbeitsspeicher	4 GB RAM
Freier Festplattenspeicher	40 GB

Betriebssystem	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1 <p>Linux Betriebssysteme</p> <ul style="list-style-type: none"> • 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	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Microsoft .NET Framework Version 4.7.2 oder höher • Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.7.2 und den Role Services: <ul style="list-style-type: none"> • 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 <p>Linux Betriebssysteme</p> <ul style="list-style-type: none"> • NTP - Client • Mono 5.14 oder höher • Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen: <ul style="list-style-type: none"> • mod_mono

- rewrite
- ssl (optional)

Minimalanforderungen für Anwendungsserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	8 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1 <p>Linux Betriebssysteme</p> <ul style="list-style-type: none"> • 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	<p>Windows Betriebssysteme</p> <ul style="list-style-type: none"> • Microsoft .NET Framework Version 4.7.2 oder höher • Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.7.2 und den Role Services: <ul style="list-style-type: none"> • 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 5.14 oder höher
- Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
 - mod_mono
 - rewrite
 - ssl (optional)

Unterstützte Datensysteme

Diese Sektion führt die Datensysteme auf, die durch die Konnektoren dieser One Identity Manager Version unterstützt werden.

Tabelle 35: Unterstützte Datensysteme

Konnektor	Unterstützte Datensysteme
Konnektor für Trennzeichen getrennte Textdateien	Beliebige Trennzeichen getrennte Textdateien.
Konnektor für relationale Datenbanken	Beliebige relationale Datenbanken, die ADO.NET unterstützen. i HINWEIS: Die zusätzliche Installation eines ADO.NET Datenproviders eines Drittanbieters kann erforderlich sein. Wenden Sie sich an Microsoft oder den Hersteller der relationalen Datenbank.
Generischer LDAP Konnektor	Beliebiger LDAP Version 3 konformer Verzeichnisserver. Der LDAP Konnektor erfordert, dass sich die Verzeichnisserver RFC-konform verhalten. Insbesondere sind die Anforderung von RFC 4514 (String Representation of Distinguished Names) und RFC 4512 (Directory Information Models) zu gewährleisten.

Konnektor	Unterstützte Datenysteme
	<p>i HINWEIS: Abhängig vom Schema können weitere Anpassungen bezüglich des Schemas und der Provisionierungsprozesse erforderlich sein.</p>
Web Service Konnektor	<p>Beliebige SOAP Web Services, die eine wsdl zur Verfügung stellen.</p> <p>i HINWEIS: Es kann der Web Service Assistent benutzt werden, um die Konfiguration für das Schreiben der Daten zum Web Service zu generieren. Für das Lesen und Synchronisieren der Daten sind zusätzliche Skripte erforderlich, welche die Methoden des Web Service Konnektors nutzen.</p>
Active Directory Konnektor	Active Directory, welches mit Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 ausgeliefert wird.
Microsoft Exchange Konnektor	<ul style="list-style-type: none"> • Microsoft Exchange 2010 ab Service Pack 3 • Microsoft Exchange 2013 ab Service Pack 1 • Microsoft Exchange 2016 • Microsoft Exchange Hybrid-Umgebungen
SharePoint Konnektor	<ul style="list-style-type: none"> • SharePoint 2010 • SharePoint 2013 • SharePoint 2016
SAP R/3 Konnektor	<ul style="list-style-type: none"> • SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40 SR 2, 7.41, 7.50 • SAP ECC 5.0 und 6.0 • SAP S/4HANA On-Premise-Edition
Unix Konnektor	Unterstützt werden die gängigsten Unix und Linux Derivate. Weitere Informationen finden Sie in den Spezifikationen für Authentication Services .
IBM Notes Konnektor	<ul style="list-style-type: none"> • Lotus Domino Server Version 8.0 bis Lotus Domino Server Version 9.0 • Als Client-Version wird IBM Notes Client 8.5.3 unterstützt.
Nativer Datenbankkonnektor	<ul style="list-style-type: none"> • SQL Server • Oracle Database • SQLite

Konnektor	Unterstützte Datenysteme
	<ul style="list-style-type: none"> • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA
Mainframe Konnektoren	<ul style="list-style-type: none"> • RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell Konnektor	<ul style="list-style-type: none"> • Windows PowerShell Version 3 oder höher
Active Roles Konnektor	<ul style="list-style-type: none"> • Active Roles 6.9, 7.0, 7.2
Azure Active Directory Konnektor	<ul style="list-style-type: none"> • Microsoft Azure Active Directory
SCIM Konnektor	Unterstützt werden Cloud-Anwendungen, welche die System for Cross-domain Identity Management (SCIM) Spezifikation in der Version 2.0 verstehen.
Exchange Online Konnektor	<ul style="list-style-type: none"> • Microsoft Exchange Online
G Suite Konnektor	<ul style="list-style-type: none"> • G Suite
Oracle E-Business Suite Konnektor	<ul style="list-style-type: none"> • Oracle E-Business Suite System Version 12.1 und 12.2
SharePoint Online Konnektor	<ul style="list-style-type: none"> • Microsoft SharePoint Online
One Identity Safeguard Konnektor	<ul style="list-style-type: none"> • One Identity Safeguard Version 2.5

Produktlizenzierung

Die Verwendung dieser Software wird geregelt durch den Software Transaktionsvertrag unter <http://www.oneidentity.com/legal/sta.aspx> und das SaaS Addendum unter <http://www.oneidentity.com/legal/saas-addendum.aspx>. Diese Software erfordert für den Betrieb weder einen Aktivierungs- noch einen Lizenzschlüssel.

Upgrade und Installationsanweisungen

Um One Identity Manager 8.1 erstmals zu installieren, folgen Sie den Installationsanweisungen im *One Identity Manager Installationshandbuch*. Ausführliche Anweisungen für die Aktualisierung finden Sie im *One Identity Manager Installationshandbuch*.

! **WICHTIG:** Beachten Sie die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 74.

Hinweise zur Aktualisierung des One Identity Manager

- Stellen Sie vor der Aktualisierung der One Identity Manager-Datenbank auf die Version 8.1 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.
- Für die automatische Softwareaktualisierung beachten Sie Folgendes:
 - Die reibungslose automatische Softwareaktualisierung von Version 7.0 auf die Version 8.1 funktioniert nur, wenn das Service Pack 7.0.3 installiert ist. Zusätzlich müssen die Dateien VI.Update.dll und JobService.dll installiert sein.

Fordern Sie die Dateien VI.Update.dll und JobService.dll über das Supportportal an.

Um die Dateien zu verteilen, nutzen Sie den Software Loader.

Zukünftige Service Packs der Versionen 7.0 werden die Änderungen dieser Dateien bereits enthalten. Für diesen Fall müssen Sie die Dateien dann nicht mehr separat verteilen.
 - Die reibungslose automatische Softwareaktualisierung von Version 7.1 auf die Version 8.1 funktioniert nur, wenn mindestens das Service Pack 7.1.3 installiert ist.
- One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe. Der Datenbankserver muss die extreme Transaktionsverarbeitung (XTP) unterstützen. Ist XTP nicht aktiviert, wird die Installation oder Aktualisierung nicht gestartet. Prüfen Sie, ob für den SQL Server die Eigenschaft **Extreme Transaktionsverarbeitung unterstützt** (Is XTPSupported) auf den Wert **True** gesetzt ist.

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 prüft der Configuration Wizard, ob diese Anforderungen erfüllt sind. Es werden im Configuration Wizard Reparaturmethoden angeboten, um die Datenbankdatei und die Datendateigruppe zu erstellen.

- Während der Aktualisierung einer One Identity Manager-Datenbank werden diverse Spalten zu physischen Pflichtfeldern, die bereits semantisch als Pflichtfelder definiert waren. Weitere Informationen finden Sie unter [Schemaänderungen](#) auf Seite 49.

Bei der Schemaaktualisierung mit dem Configuration Wizard kann es, aufgrund inkonsistenter Daten, zu Fehlern kommen. Die Aktualisierung wird mit einer Fehlermeldung abgebrochen.

```
<Tabelle>.<Spalte> must not be null
Cannot insert the value NULL into column '<Spalte>', table '<Tabelle>';
column does not allow nulls.
UPDATE fails
```

Prüfen und korrigieren Sie vor der Aktualisierung einer One Identity Manager-Datenbank die Daten. Im Add-on für das Konfigurationsmodul auf dem Installationsmedium wird ein Prüfskript bereitgestellt (`\SDK\SQLSamples\Files\MSSQL2K\30374.sql`). Im Fehlerfall korrigieren Sie die Daten und starten Sie die Aktualisierung erneut.

- Während der Installation einer neuen One Identity Manager-Datenbank mit der Version 8.1 oder der Aktualisierung einer One Identity Manager-Datenbank von den Versionen 7.0, 7.1 oder 8.0 auf die Version 8.1 können Sie festlegen, ob Sie mit abgestuften Berechtigungen auf Serverebene und Datenbankebene arbeiten möchten. Dabei werden durch den Configuration Wizard SQL Server Anmeldungen und Datenbankbenutzer mit den erforderlichen Berechtigungen für den administrative Benutzer, Konfigurationsbenutzer und Endbenutzer erstellt. Ausführliche Informationen zu den Berechtigungen finden Sie im *One Identity Manager Installationshandbuch*.

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 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.

- Damit die Kompilierung von HTML-Anwendungen mit dem Configuration Wizard erfolgreich durchgeführt werden kann, müssen Pakete aus dem NPM-Repository

heruntergeladen werden. Stellen Sie daher sicher, dass die Arbeitsstation, auf der der Configuration Wizard ausgeführt wird, eine Verbindung zur Webseite <https://registry.npmjs.org> herstellen kann.

Alternativ ist es möglich, die Pakete von einem Proxy-Server herunterzuladen und manuell zur Verfügung zu stellen. Weitere Informationen finden Sie im Knowledge Artikel unter <https://support.oneidentity.com/kb/266000>.

- In den One Identity Manager Versionen 8.0, 8.0.1 und 8.0.2 wurden bei der One Identity Manager History Database-Installation der One Identity Manager History Service und der One Identity Manager Service gleichzeitig installiert.


Wenn Sie von diesem Problem betroffen sind, deinstallieren Sie vor der Aktualisierung Ihrer One Identity Manager History Database-Installation den One Identity Manager History Service. Führen Sie in der Kommandozeile im administrativen Kontext folgenden Aufruf aus:

```
sc delete "HDBService"
```

Aktualisieren des One Identity Manager auf Version 8.1

- WICHTIG:** Beachten Sie die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 74.

Um eine bestehende One Identity Manager Installation auf die Version 8.1 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.

- HINWEIS:** Um eine One Identity Manager History Database Installation zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.

- 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. (von Version 7.0.x oder Version 7.1.x) Beenden Sie den One Identity Manager Service auf dem Server, der die direkten Anfragen der Datenbank verarbeitet.
(von Version 8.0.x) 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 **130** 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 und folgen Sie den Anweisungen.

7. (von Version 7.0.x oder Version 7.1.x) Aktualisieren Sie den One Identity Manager Service auf dem Server, der die direkten Anfragen der Datenbank verarbeitet.
(von Version 8.0.x) 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.

! **HINWEIS:** Um eine One Identity Manager History Database Installation zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.

- 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. Wenn der One Identity Manager Service ursprünglich nicht das lokale Systemkonto zur Anmeldung nutzte, stellen Sie die ursprüngliche Einstellung wieder her. 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.

Um Synchronisationsprojekte auf die Version 8.1 zu aktualisieren

1. Wenn Sie Synchronisationsprojekte für die Anbindung von Cloud-Anwendungen im Universal Cloud Interface eingerichtet haben, aktualisieren Sie in diesen Synchronisationsprojekten das Zielsystemschemata. Verwenden Sie den Synchronization Editor.
2. 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.

Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 79.

Um einen Anwendungsserver auf die Version 8.1 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 verwenden Sie den Eintrag **Update immediately** im Menü des angemeldeten Benutzers.

Um das Web Portal auf die Version 8.1 zu aktualisieren

HINWEIS: Stellen Sie sicher, dass der Anwendungsserver aktualisiert ist, bevor Sie das Web Portal aktualisieren. Ab Version 7.1 benötigt das Web Portal einen Anwendungsserver mit installiertem Suchdienst.

- 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.

- Um das Web Portal manuell zu aktualisieren, deinstallieren Sie die bestehende Web Portal Installation und installieren Sie das Web Portal neu. Ausführliche Anweisungen finden Sie im *One Identity Manager Installationshandbuch*.

Um das Web Portal für Betriebsunterstützung auf die Version 8.1 zu aktualisieren

1. Deinstallieren Sie das Web Portal für Betriebsunterstützung.
2. Installieren Sie einen API Server und kompilieren Sie die HTML-Anwendung **Operations Support Portal**. Ausführliche Anweisungen finden Sie im *One Identity Manager Installationshandbuch*.

Um die Manager Webanwendung auf die Version 8.1 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 Bearbeitungsrechte auf das Installationsverzeichnis der Manager Webanwendung. Prüfen Sie, ob die entsprechenden Rechte vorhanden sind.

Anwenden von Patches für Synchronisationsprojekte

⚠ VORSICHT: Patches ändern keine kundenspezifischen Anpassungen in den Synchronisationsprojekten. Dennoch können Konflikte auftreten, wenn Patches auf ein Synchronisationsprojekt mit kundenspezifischen Anpassungen angewendet werden. Möglicherweise kann das zu Datenverlust führen.

Bevor Sie einen Patch anwenden

1. Prüfen Sie anhand der Patchbeschreibung, ob der Patch notwendige Verbesserungen für das Synchronisationsprojekt bereitstellt.
2. Prüfen Sie, ob Konflikte mit kundenspezifischen Anpassungen auftreten können.
3. Erstellen Sie eine Datenbanksicherung, um im Bedarfsfall den ursprünglichen Zustand wieder herstellen zu können.
4. Deaktivieren Sie das Synchronisationsprojekt.

ℹ HINWEIS: Wenn Sie Synchronisationsprojekte für die Anbindung von Cloud-Anwendungen im Universal Cloud Interface eingerichtet haben, aktualisieren Sie in diesen Synchronisationsprojekten das Zielsystemschemata, bevor Sie die Patches anwenden. Verwenden Sie den Synchronization Editor.

Um Patches anzuwenden

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie das Menü **Bearbeiten | Synchronisationsprojekt aktualisieren**.
3. Wählen Sie im Bereich **Verfügbare Patches** den Meilenstein aus, der angewendet werden soll.

Im Bereich **Details - Installationszusammenfassung** werden alle abhängigen Patches in der Reihenfolge angezeigt, in der sie angewendet werden.

4. Klicken Sie **Ausgewählte Patches anwenden**.
5. Wenn Benutzereingaben angefordert werden, erfassen Sie die benötigten Daten.
6. (Optional) Wählen Sie im Bereich **Verfügbare Patches** die Patches für neue Funktionen aus, die angewendet werden sollen. Mehrfachauswahl ist möglich.
Im Bereich **Details - Installationszusammenfassung** werden die Patches in der Reihenfolge angezeigt, in der sie angewendet werden.
7. Klicken Sie **Ausgewählte Patches anwenden**.
8. Wenn Benutzereingaben angefordert werden, erfassen Sie die benötigten Daten.
9. Prüfen Sie anhand des Patchprotokolls, ob kundenspezifische Anpassungen nachbearbeitet werden müssen.
10. Falls erforderlich, überarbeiten Sie die kundenspezifischen Anpassungen in der Synchronisationskonfiguration.
11. Führen Sie eine Konsistenzprüfung durch.
12. Simulieren Sie die Synchronisation.
13. Aktivieren Sie das Synchronisationsprojekt.
14. Speichern Sie die Änderungen.

HINWEIS: Ein Patch wird erst dann wirksam, wenn die damit angewendeten Änderungen in der Datenbank gespeichert wurden. Wenn die Konsistenzprüfung oder die Simulation Fehler ergeben, die nicht behoben werden können, können Sie die Anwendung des Patches rückgängig machen, indem Sie das Synchronisationsprojekt neu laden ohne die Änderungen zu speichern.

Ausführliche Informationen zum Aktualisieren von Synchronisationsprojekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Siehe auch:

- [Änderungen an Synchronisationsvorlagen](#) auf Seite 57
- [Patches für Synchronisationsprojekte](#) auf Seite 58

Prüfen der erfolgreichen Installation

Um festzustellen, ob die Version installiert ist

- Starten Sie den Designer oder den Manager und wählen Sie den Menüeintrag **Hilfe | Info**.

Auf dem Tabreiter **Systeminformationen** erhalten Sie einen Überblick über Ihre Systemkonfiguration.

Die Versionsnummer 2019.0001.0021.0000 für alle Module und die Anwendungsversion 8.1 2019-01-21-031 weisen darauf hin, dass diese Version installiert ist.

Zusätzliche Ressourcen

Zusätzliche Informationen sind verfügbar unter:

- [One Identity Manager Support](#)
- [One Identity Manager Online-Dokumentation](#)
- [Identity and Access Management Community](#)
- [One Identity Manager Trainingsportal](#)

Weltweite Verwendung

Dieser Abschnitt enthält Informationen über die Installation und die Verwendung dieses Produkts in anderen als englischen Konfigurationen, wie etwa denen, die von Kunden außerhalb von Nordamerika benötigt werden. Dieser Abschnitt ersetzt jedoch nicht die Informationen zu den unterstützten Plattformen und Konfigurationen, die an anderen Stellen in der Dokumentation beschrieben sind.

Diese Version ist Unicode-fähig und unterstützt jeden Zeichensatz. Sie unterstützt den simultanen Betrieb mit mehrsprachigen Daten. Diese Version unterstützt die Verwendung der Software in den folgenden Regionen: Nordamerika, Westeuropa und Lateinamerika, Mittel- und Osteuropa.

Diese Version ist in folgenden Sprachen lokalisiert: Deutsch

Diese Version hat die folgenden bekannten Fähigkeiten oder Einschränkungen: Andere Sprachen, die für das Web UI bestimmt sind, werden über das Produkt One Identity Manager Language Pack bereitgestellt.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Copyright 2019 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.




Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter <http://www.OneIdentity.com/legal/patents.aspx>.

Marken

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

Legende

-  **WARNUNG:** Das Symbol **WARNUNG** weist auf mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.
-  **WICHTIG, HINWEIS, TIPP, MOBIL, or VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.