

One Identity Manager 8.1.1

Versionshinweise

Juli 2019

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 8.1.1 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 8.1 aufgeführt.

One Identity Manager 8.1.1 ist ein Patch Release mit neuen Funktionen und verbessertem Verhalten. Siehe [Neue Funktionen](#) auf Seite 3 und [Verbesserungen](#) auf Seite 6.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.1 ist, lesen Sie auch die Versionshinweise der vorangegangenen Versionen. Die Versionshinweise sowie Versionshinweise zu zusätzlichen Modulen, die auf der One Identity Manager-Technologie basieren, finden Sie unter [One Identity Manager Support](#).

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 8.1.1

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 8.1.1.

Basisfunktionen

- Verwaltete Instanzen in Azure SQL-Datenbank werden unterstützt.
Um die One Identity Manager-Datenbank in einer verwalteten Instanz in Azure SQL-Datenbank zu betreiben, wird der Tarif **Unternehmenskritisch** benötigt.
Ausführliche Informationen zu den Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank im One Identity Manager finden Sie im *One Identity Manager Installationshandbuch*. Ausführliche Informationen zum Tarif finden Sie bei Microsoft unter <https://azure.microsoft.com/en-us/services/sql-database/>.
- Windows Server 2019 wird für Dienstserver, Webserver und Anwendungsserver unterstützt.
- Über die Konfigurationsparameter **Common | MailNotification | DefaultFont** und **Common | MailNotification | DefaultFontSize** können Schriftart und Schriftgröße für Mailvorlagen im Mailvorlageneditor festgelegt werden.
- In Mailvorlagen sind beliebige Parameter beim Skriptaufruf erlaubt.
Syntax: `$SCRIPT(ScriptName, "Options")$`
Der Options-Parameter ist optional und wird als String übergeben. Kundenspezifische Parameter können in beliebiger Weise in diesem String kodiert werden. Die Anführungszeichen ("") werden dabei per Verdopplung maskiert. Im Skript wird der Parameter dabei als zweiter Parameter nach dem Basisobjekt angegeben. Das Basisobjekt kann jetzt entweder IEntity oder ISingleDbObject sein.
- Das **RequestWatchDogPlugin** besitzt einen neuen Parameter **Aktion** (Action) um festzulegen, welche Aktion ausgeführt werden soll, wenn es zum Stillstand der Anfragen kommt. Zulässige Werte sind **Restart** (Standard) und **Log**.

Webanwendungen

- One Identity bietet nun Benutzern die Möglichkeit, sich mithilfe von (physischen) Sicherheitsschlüsseln bequem und sicher an den Webanwendungen des One Identity Managers anzumelden. Diese Sicherheitsschlüssel unterstützen den W3C-Standard **Webauthn**. Die Nutzung dieser Sicherheitsschlüssel gewährleistet eine höhere Sicherheit beim Anmelden.

Neue Web Designer-Konfigurationsschlüssel:

- VI_Common_AccessControl_Webauthn_2FAID
- VI_Common_AccessControl_Webauthn_2FA_VisibleControls
- VI_Employee_QERWebAuthnKey_Filter
- VI_Common_AccessControl_Webauthn_2FA

Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*, im *One Identity Manager Konfigurationshandbuch für Webanwendungen* und im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

- Es ist nun möglich mit Hilfe dreier Web Designer-Konfigurationsschlüssel das Eingabeformat für Datums- sowie Zeitangaben für das gesamte Webprojekt festzulegen.

Neue Web Designer-Konfigurationsschlüssel:

- VI_Common_InputFormat_DateTime
- VI_Common_InputFormat_Date
- VI_Common_InputFormat_Time

Weitere Informationen zu den Wertformaten finden Sie unter

<https://docs.telerik.com/kendo-ui/framework/globalization/dateformatting>.

- Die Nutzungsbedingungen werden jetzt automatisch in der Sprache angezeigt, die für das Web Portal genutzt wird.

Zielsystemanbindung

- Mit Synchronisationsprojekten für Personendaten aus dem Human Resources Modul einer Oracle E-Business Suite können nun auch Abteilungen und ihre Zuordnungen zu Personen synchronisiert werden. Dafür werden mit der Standardsynchronisationsvorlage zwei neue Mappings bereitgestellt.

Zusätzlich unterstützt der Oracle E-Business Suite Konnektor auch Hierarchiefilter für Organisationshierarchien. Die zu synchronisierenden Abteilungen können im Scope der Synchronisationsprojekte per Hierarchiefilter aus allen Organisationen gefiltert werden.

Abteilungen können außerdem durch ihren Typ von anderen Organisationen unterschieden werden. Da diese Typen in der Oracle E-Business Suite kundenspezifisch definiert werden können, werden die Abteilungen in den Standardmappings nicht nach dem Typ gefiltert. Um Abteilungen über ihren Typ zu filtern, definieren Sie eine eigene Schemaklasse.

- **HINWEIS:** Die neuen Standardmappings stehen nur in Synchronisationsprojekten zur Verfügung, die mit dem One Identity Manager 8.1.1 neu erstellt wurden. Es wird kein Patch für diese Änderung bereitgestellt.

Um diese Funktionalität in bestehenden Synchronisationsprojekten anwenden zu können, aktualisieren Sie das Zielsystemschemata in diesen Projekten. Damit stehen die beiden neuen Schematypen HROrganization und HRPersonInOrganization zur Verfügung. Definieren Sie für diese Schematypen eigene Schemaklassen und eigene Mappings.

- One Identity Safeguard Version 2.6 und Version 2.7 werden unterstützt.

Es werden Patches für Synchronisationsprojekte mit den Patch ID's VPR#31459, VPR#31664A, VPR#31664B, VPR#31703, VPR#31775A und VPR#31775B bereitgestellt.

- Verbesserte Unterstützung von One Identity Safeguard Clustern beim Verbindungsaufbau.

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31569 bereitgestellt. Wenn Sie One Identity Safeguard Cluster verwenden, sollte nach dem Anwenden des Patches der Systemverbindungsassistent erneut ausgeführt werden, um die Appliances des Clusters zu ermitteln.

- Die Genehmiger von Zugriffsanforderungsrichtlinien werden initial automatisch die Eigentümer der PAM Assets, PAM Assetkonten, PAM Verzeichniskonten, PAM Assetgruppen und PAM Kontogruppen. Diese Zuordnung erfolgt einmalig, wenn zu einem PAM Objekt eine Zugriffsanforderungsrichtlinie ermittelt werden kann. Je Zugriffsanforderungsrichtlinie wird eine neue Anwendungsrolle für die Eigentümer unter der Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** erstellt.

Eine Anwendungsrolle für die Eigentümer wird einem PAM Objekt nur automatisch zugewiesen, wenn dem PAM Objekt noch keine Anwendungsrolle zugewiesen ist. Eine bestehende Zuweisung wird nicht geändert. Ändern Sie bei Bedarf die Anwendungsrolle manuell.

- Microsoft Exchange 2019 mit kumulativem Update 1 und Microsoft Exchange 2016 mit kumulativem Update 12 werden unterstützt.
- Microsoft Exchange verknüpfte Raumpostfächer werden unterstützt.

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30964 bereitgestellt.

- Der One Identity Manager unterstützt bei der Auflösung der Zentralen Benutzerverwaltung einer SAP R/3-Umgebung. Dabei werden das Zentralsystem und die Tochtersysteme so herausgelöst, dass sie anschließend als eigenständige Mandanten mit dem One Identity Manager verwaltet und unabhängig voneinander administriert werden können.

Es können sowohl nur einzelne Mandanten aus der Zentralen Benutzerverwaltung herausgelöst als auch die gesamte Zentrale Benutzerverwaltung aufgelöst werden.

Ein Anleitung zur Auflösung der Zentralen Benutzerverwaltung erhalten Sie über den Support. Das Support Portal ist unter <https://support.oneidentity.com/identity-manager/> erreichbar.

- Es wird eine rezertifizierte Version des One Identity Manager Business Application Programming Interface (BAPI) ausgeliefert. Das BAPI hat einen zu Gunsten der Performance reduzierten Funktionsumfang. Das BAPI ist nicht mehr kompatibel zu One Identity Manager Version 6.1.x oder älteren Versionen.

Die Funktionen des BAPI werden sowohl als Add-On Assembly Kit (AAK)-Paket, als Transport vom Kopieren und jetzt als Workbench Transport bereitgestellt. Der Importweg kann frei gewählt werden. Das Coding ist identisch.

- SharePoint 2019 wird unterstützt.
- Die Ausführung der Prozesse zur Provisionierung und Einzelobjektsynchronisation sowie einzelner zielsystemspezifischer Prozesse kann auf verschiedene Jobserver

verteilt werden. So wird die Verarbeitung der Objekte parallelisiert und der Gesamtprozess beschleunigt.

Für die Verteilung werden alle Server genutzt, denen die am Basisobjekt hinterlegte Serverfunktion zugewiesen ist.

Ausführliche Informationen zur Lastverteilung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation* und in den einzelnen Zielsystemhandbüchern.

- **TECH PREVIEW ONLY:** Es wird ein neuer LDAP Konnektor **LDAP Connector (Version 2 - Tech Preview)** zur Verfügung gestellt. Es werden keine Mappings und keine Projektvorlage zur Verfügung gestellt. Dieser Konnektor kann in Testumgebungen getestet werden. Verwenden Sie den Konnektor auf keinen Fall in einer produktiven Umgebung.

Identity Management und Access Governance

- Unterstützung einer Peer-Gruppen-Analyse für Bestellungen.

Es gibt ein neues Ereignis `PeerGroupAnalysis` an der Tabelle `PersonWantsOrg`, welches über einen **EX** Schritt in den Genehmigungsworkflow eingebunden werden kann. Das Ereignis prüft die Trefferquote innerhalb der Peer-Gruppe des Bestellempfängers und/oder Funktionsfremdheit der bestellten Berechtigung und der Abteilung des Empfängers. Trefferquote und Funktionsfremdheit werden an der Bestellung vermerkt und der Schritt in Abhängigkeit vom Ergebnis als genehmigt oder abgelehnt beendet.

Die Konfiguration der Peer-Gruppen-Analyse erfolgt über den Konfigurationsparameter **QER | ITShop | PeerGroupAnalysis** und seine untergeordneten Konfigurationsparameter.

Siehe auch:

- [Verbesserungen](#) auf Seite 6
- [Gelöste Probleme](#) auf Seite 11
- [Schemaänderungen](#) auf Seite 29
- [Patches für Synchronisationsprojekte](#) auf Seite 32

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die im One Identity Manager 8.1.1 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Performanceverbesserung bei der Überprüfung von Spalten, die laut Defini-	31263,

Verbesserung	Fehler ID
tion in der Tabelle QBMUniqueGroup eindeutig sein müssen.	31648
Performanceverbesserungen im DBQueue Prozessor.	31293
Performanceverbesserung bei der Verarbeitung von Transaktionen, die wiederholt Aufträge in die DBQueue einstellen.	31490
Im Konfigurationsparameter Common MailNotification Signature LinkDisplay kann ein alternativer Anzeigetext für den Link zur Firmenwebseite für die Verwendung in der E-Mail Signatur festgelegt werden.	19852
Verbesserungen im Job Queue Info. <ul style="list-style-type: none"> Bei der Anzeige des Protokolls für einen Jobserver wird der Port berücksichtigt. Für die Statusabfrage von Jobservern kann über das Kontextmenü Anmeldeinformationen eintragen ein Benutzer und das Kennwort des Benutzer angegeben werden. 	22926, 30711
Unterstützung des System Debugging auf 64-Bit Systemen.	31203
Verbesserte Überprüfung von Anmeldungen. Über den Konfigurationsparameter Common Authentication SessionsPerUserAndMinute kann die Anzahl der Sitzungen, die ein Benutzer innerhalb kurzer Zeit öffnen darf, festgelegt werden. Standardwert ist 10 . Ist die Anzahl überschritten, erhält der Benutzer eine Meldung.	31321
Über den Konfigurationsparameter QBM DBQueue GenProcIDReplaceLimit kann ein Grenzwert für Prozessersetzungen definiert werden.	31423
Aktualisierung von Drittanbieterkomponenten.	31443, 31444, 31446, 31318
Verbesserte Absicherung der API des One Identity Manager Service.	31542
Verbesserte Absicherung der API des Anwendungsservers.	31553, 31564
Verbesserter Schutz vor potentiell schädlichen SQL Ausführungen.	31652
Performanceverbesserung in der Prozedur QBM_PGUIDReplacelight.	31676

Tabelle 2: Allgemein Webanwendungen

Verbesserung	Fehler ID
Im Web Portal werden unter Verantwortlichkeiten Meine Verantwortlichkeiten One Identity Manager Anwendungsrollen sämtliche Anwendungsrollen verwaltet, für die man verantwortlich ist.	797112

Verbesserung	Fehler ID
Im Web Portal können Benutzer über Mein Profil Persönliche Daten Sprache zur Wertformatierung festlegen, wie Datums- und Zahlenformate formatiert werden sollen.	796853
Verbesserte Fehlermeldung, wenn für Delegierungen keine Entscheidungsrichtlinie vorhanden ist.	30656
Um zu verhindern, dass Sitzungen von Benutzern gestohlen werden können, wird die Session ID nun im HTML-Code nicht mehr ausgegeben. Die Webanwendung muss dafür im Release-Modus laufen.	31656
Verbesserte Sicherheit im Umgang mit Spaltenfiltern.	31754

Tabelle 3: Zielsystemanbindung

Verbesserung	Fehler ID
Performanceverbesserung beim Nachladen von Objekten aus der Datenbank.	31404
Wenn für eine Schemaeigenschaft die Option Ignoriere nicht-definierte Werte aktiviert ist, erscheint eine Meldung im Synchronisationsprotokoll, wenn ein Konnektor versucht, einen nicht definierten Wert zu schreiben.	30522
Operationen für Mitgliedschaften werden im Synchronisationsprotokoll umfangreicher aufgezeichnet.	31851
Wurde in einem Synchronisationsprojekt das Konnektorschema mittels einer Schemaerweiterungsdatei erweitert, kann die Schemaerweiterung nach dem Speichern der Zielsystemverbindung im Systemverbindungsassistenten betrachtet und bearbeitet werden.	31773, 31833
Die Zugriffsbeschränkung für die Azure Active Directory Schemaeigenschaft User.CompanyName wurde entfernt. CompanyName ist nun schreibbar. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31456 bereitgestellt.	31456
Verbesserte Gruppierung von Azure Active Directory Benutzerkonten im Manager.	31803
Performanceverbesserung bei der Provisionierung von Active Directory Gruppen, Containern und Domänen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31419 bereitgestellt.	31419
Performanceverbesserung durch Korrektur von Objektfiltern in der Active Directory Projektvorlage. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31792 bereitgestellt.	31792
Zur Lastverteilung der Prozesse zur Provisionierung und Einze-	30886

lobjektsynchronisation sowie einzelner zielsystemspezifischer Prozesse auf verschiedene Jobserver wurde das Verhalten der Active Directory Prozesse angepasst.

HINWEIS: In diesem Zusammenhang wurde das Skript ADS_GetQBMServer angepasst. Prüfen Sie die kundenspezifische Verwendung oder Überschreibungen des Skriptes.

Wenn Sie das Skript ADS_GetQBMServer kundenspezifisch überschrieben haben, wird es weiter verwendet jedoch die Funktion zur Lastverteilung nicht genutzt. Wenn Sie die Lastverteilung einsetzen möchten, passen Sie das Skript entsprechend an oder verwenden Sie das Standardskript.

Performanceverbesserung beim Laden von Synchronisationsobjekten aus einer Microsoft Exchange-Umgebung, wenn die Revisionsfilterung genutzt wird. 31165

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31165 bereitgestellt.

Performanceverbesserung beim Laden von Synchronisationsobjekten aus einer Exchange Online-Umgebung, wenn die Revisionsfilterung genutzt wird. 31166

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31166 bereitgestellt.

Performanceverbesserung bei der Provisionierung von Notes Richtlinien und Zertifikaten. 31420

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31420 bereitgestellt.

Performanceverbesserung bei der Provisionierung von SAP Benutzerkonten. 31412

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31412 bereitgestellt.

Performanceverbesserung beim Löschen von Mitgliedschaften in SAP Rollen. 31235

Verbesserter Split-Algorithmus im SAP Konnektor bei sehr langen Where-Klauseln in externen Schemaerweiterungen. 31834

Der LDAP Konnektor unterstützt Schemas mit Inhalten, die Base64-kodiert sind. 28647

Der LDAP Konnektor unterstützt das Auslesen von Attributen von Hilfsklassen, die über das auxiliaryClass-Attribut im objectClass-Schema zugewiesen wurden. 31483

Der LDAP Konnektor behandelt Einträge, die nicht RFC-konform sind, toleranter. 31548, 31873

Verbesserung	Fehler ID
<p>Mit dieser Änderung werden nun nicht RFC 4514 konforme unmaskierte führende und hängende Leerzeichen als nicht signifikant, das heißt nicht mehr zum Namen gehörend, behandelt. Alle laut RFC nicht erlaubten Leerzeichen werden nun normalisiert. Andere nicht RFC-konforme Einträge werden ignoriert und Warnungen im Protokoll ausgegeben.</p> <p>i HINWEIS: Auf einigen LDAP Systemen können Schreiboperationen auf Einträge, die nicht RFC-konform sind, Fehlerzustände verursachen.</p>	
Der RACF Konnektor unterstützt die Hilfsklasse RacfUserCsdataSegment.	31356
Die Prozessfunktion RunAgent der Prozesskomponente NDO Component wurde um zusätzliche Parameter vom Typ OUT erweitert.	31030
Über den Konfigurationsparameter TargetSystem SAPR3 Accounts CalculateLicence kann festgelegt werden, ob die Berechnung der SAP Systemvermessung für SAP Benutzerkonten ausgeführt wird.	31204
Performanceverbesserung bei der Synchronisation von SAP Kostenstellen.	31543
Performanceverbesserung durch Korrektur von Objektfiltern in der SAP Projektvorlagen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31796 bereitgestellt.	31796
Der SCIM Konnektor unterstützt die Übergabe eines gewünschten Scope für das per OAuth 2.0 angeforderte Zugriffstoken. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31756 bereitgestellt.	31756
Performanceverbesserung durch Korrektur von Scopefiltern in den Oracle E-Business Suite Projektvorlagen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31794 bereitgestellt.	31794

Tabelle 4: Identity Management und Access Governance

Verbesserung	Fehler ID
Verbesserte Prozessüberwachung von Bestellungen. Über den Konfigurationsparameter Common ProcessState UseGenProcIDFromPWO kann gesteuert werden, ob die GenProcID einer IT Shop Bestellung über die gesamte Zeit eines Genehmigungsprozesses beibehalten wird.	31418
Die Dokumentation zur Vererbung von Unternehmensressourcen über Systemrollen und die Wirkung von Ausschlussdefinitionen wurde umfassend überarbeitet (<i>One Identity Manager Administrationshandbuch für Systemrollen</i>).	28312

Verbesserung	Fehler ID
Performanceverbesserung bei der Verarbeitung der Bestellungen von Entscheidern, die automatisch genehmigt werden.	31341
Performanceverbesserung beim Löschen von Kunden mit Bestellungen aus dem IT Shop.	31668
Performanceverbesserung beim Umzug von Bestellungen.	31597
Das Erinnerungsintervall und das Timeout für Entscheidungsschritte für Attestierungsvorgänge werden standardmäßig alle 30 Minuten geprüft. Das Prüfintervall kann über den Zeitplan Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen festgelegt werden.	31383

Siehe auch:

- [Schemaänderungen](#) auf Seite 29
- [Patches für Synchronisationsprojekte](#) auf Seite 32

Gelöste Probleme

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

Tabelle 5: Allgemein

Gelöstes Problem	Fehler ID
Die Prozedur QBM_PDBQueueOverviewFill aktualisiert die Tabelle DBQueueOverview zu häufig.	31217, 31296
Fehler bei der DBQueue Prozessor Verarbeitung: Divide by zero error encountered.	31924, 31925
Falsche Werte in DialogCountry.NumericCode.	31352
Beim Schreiben von CSV-Dateien, die nur einen Header enthalten, fehlt der abschließende Zeilenumbruch.	31556
DialogTree.ConfigurationFlags ist nicht kundenspezifisch änderbar.	31393
Der Database Compiler setzt den Status Warten auf Kompiler zu zeitig. Beim vorzeitigen manuellen Abbruch des Compilers wird der Status nicht entfernt.	31408
Umgebungsvariablen im Prozessparameter FileName der Prozessfunktion DumpResult der Prozesskomponente SQLComponent werden zur Ausführungszeit nicht ersetzt.	31513
Fehler in der deutschen Übersetzung für DBQueue Aufträge.	31117

Gelöstes Problem	Fehler ID
Sind in einer One Identity Manager History Database kundenspezifische Tabellen vorhanden, schlägt die Migration fehl.	31530
Die Rechtegruppe CCCEditPermissions besitzt unzureichende Berechtigungen zum Erstellen von Objekten für Standardtabellen mit kundenspezifischen Spalten.	31431
In CustomProperty*-Spalten ist die Eingabe von @ nicht möglich.	31593
Die Prozedur QBM_PUserDetectByGroupList entfernt zu viele Rechtegruppen.	31601
Fehler String or binary data would be truncated während der Aktualisierung des One Identity Manager auf Version 8.1.	31617, 31663
Während der Aktualisierung des One Identity Manager auf Version 8.1 werden kundendefinierte Trigger gelöscht.	31658
Die Prozedur QBM_PDeleteDeep hinterlässt unter Umständen deaktivierte Trigger.	31677
Fehler bei der Ausführung der Konsistenzprüfung GUID in primary key with invalid format für die Tabelle JobQueueStats.	31688
Die Konsistenzprüfung QBMLock has no entry but XMarkedForDeletion is set gibt die Tabelle nicht mit aus.	31860
Die Konsistenzprüfungen QBMLock has no entry but XMarkedForDeletion is set und QBMLock has entry without XMarkedForDeletion set liefern für ReadOnly-Tabellen falsche Ergebnisse. Beim Ausführen der Reparaturmethode tritt ein Fehler auf.	31799
Swagger-Definition in der API-Dokumentation des Anwendungsservers enthält nicht abgeschlossenes XML.	31713
Im Suchindex werden unter Umständen nicht alle Elemente indiziert.	31881
Die Prozessfunktion CSVExport der Prozesskomponente ScriptComponent schreibt Header mehrfach.	31731
Falsche Transliteration von Đ(U0110) und đ(U0111) im Skript VID_TransliterateDiacritics.	31737
Fehlermeldung im HistoryDB Manager, wenn für Spalten, die nicht zur Aufzeichnung von Änderungen konfiguriert sind, Aufzeichnungen in der One Identity Manager History Database existieren.	31631
Fehler bei der Ausführung des Berichtes über die Systemkonfiguration Divide by zero error encountered für die Werte AVG latency write und AVG latency write TempDB .	31610
Fehler beim Speichern eines neu angelegten Skriptes mit dem System Debugger in die One Identity Manager-Datenbank.	31786

Gelöstes Problem	Fehler ID
Für DialogColumn.ColumnName mit einer Länge von 29 oder 30 Zeichen ist die Variable @ColumnName in QBM_ZSplittedLookupFill zu kurz.	31840
In der Prozessgenerierung ist es möglich, dem Basisobjekt der Generierung (Entity) ein neues Objekt zuzuweisen.	31854
<p>i HINWEIS: Sollten Sie diese Funktionalität genutzt haben, werden Fehlermeldungen bei der Kompilierung der Prozesse ausgegeben. Korrigieren Sie Ihre Prozesse.</p>	
Alle Datenbanken in einer AlwaysOn-Verfügbarkeitsgruppe erhalten dieselbe UniqueDatabaseId.	31866
SingleDbObjectSnapshot maskiert XML-Sonderzeichen nicht, wenn der Wert verschlüsselt ist.	31869

Tabelle 6: Allgemein Webanwendungen

Gelöstes Problem	Fehler ID
Probleme bei der Sprachauswahl, wenn der One Identity Password Manager aus dem Web Portal gestartet wird.	29035
Im Kennworrücksetzungsportal werden die Informationen zur Kennwortstärke nicht sprachabhängig angezeigt.	30694
Die Filtereinstellungen für Datumsspalten sind im Web Portal nur auf Englisch verfügbar.	31118
Beim Export eines Berichtes wird nicht die individuelle Vorlage, sondern die Standardvorlage verwendet.	31231
Für einen Menüeintrag mit einer Weiterleitung auf eine externe URL und den Optionen In neuem Frame öffnen und Werkzeugleisten anzeigen wird im Web Portal die Werkzeugleiste im Popup-Fenster nicht angezeigt.	31384
Verstößt man beim Ändern des Kennworts gegen die Kennwortrichtlinie, wird statt der Kennwortrichtlinie eine Fehlermeldung angezeigt.	30389
Im generierten Code des API Clients sind nicht alle Typen vorhanden.	799497
Die Web Designer-Komponente VI_Common_ExternalFormHost wurde geändert. Sie kann nicht mehr dazu verwendet werden, um beliebige URLs anzuzeigen. Falls Sie diese Funktionalität benötigen, müssen Sie existierenden Code umbauen, um die Formularkomponente QBM_Common_ExternalFormHost zu verwenden. Diese bietet den Vorteil, dass URLs nicht in Form von URL-Parametern übergeben werden.	800060
Die Web Designer-Komponente VI_Common_UserMessageAdd kodiert den eingegebenen Text aus Sicherheitsgründen nun standardmäßig nach HTML. Sie können dieses Verhalten mithilfe der virtuellen Funktion <code>DoNotHtmlEncode()</code> beim Aufruf der Komponente abschalten.	800062

Gelöstes Problem	Fehler ID
Im Web Portal können Berichtsabonnements ohne Wert im Pflichtfeld gespeichert werden.	31058
Im Web Portal werden in der Historie für Änderungen einer Person die Datumsangaben im UTC-Format angezeigt.	31434
Im Web Portal wird das Gültig bis-Datum mit Uhrzeiten nach 23:59 Uhr im Warenkorb falsch übernommen.	31484
Die Web Designer-Komponente VI_Edit_MultiLimitedValues selektiert in der Filterbedingung Werte aus dem falschen Attribut.	31505
Die Gültigkeit eines Kennwortes wird bei Verbindung des Kennwortrücksetzungsportals über den Anwendungsserver erst beim Speichern geprüft.	31354
Historisierte Daten aus One Identity Manager Version 6 werden im Web Portal nicht korrekt angezeigt.	31523
Schreibgeschützte Werte für Attestierungsfälle können im Web Portal geändert werden.	31603
Unter bestimmten Umständen kommt es beim Anzeigen der Herkunft einer Mitarbeiterberechtigung im Web Portal zum Fehler.	31638
Für einige Objekte (beispielsweise VI_ITShop_DeleteItemFromCart) können im Web Designer keine Erweiterungen angelegt werden.	31504
Unter bestimmten Umständen friert das Web Portal beim Exportieren von Daten ein.	31295
Unter bestimmten Umständen wird im Web Designer für die manuelle WCF-Verbindung das anzuklickende Schlüsselsymbol nicht kontinuierlich eingeblendet.	31525
Unter bestimmten Umständen friert im API Designer bei NPM-Vorgängen der Database Compiler ein.	31723
Sehr lange Wartezeit im Internet Explorer bis im Web Portal das Formular zur Zuweisung einer Systemberechtigung an einen Eigentümer angezeigt wird.	31037
Unter bestimmten Umständen werden im Web Portal auf der Produktauswahlseite nicht alle Produktkategorien angezeigt.	31818
Unter bestimmten Umständen tritt bei der Analyse von Attestierungsfällen der Fehler auf: Das Objekt vom Typ UNSAccount existiert nicht in der Datenbank oder Sie haben keine Rechte es zu sehen.	31842
Im Internet Explorer und Microsoft Edge werden Berichte unter Umständen nicht korrekt dargestellt	31896

Gelöstes Problem	Fehler ID
Fehler beim Freigeben der Standardwebanwendung im Release-Modus: Der Wert darf nicht NULL sein.	31931
Die Suche am Grid ist nicht ausblendbar. Der Wert false für die Variable IsSearchActive in der Erweiterung eines Grids wird nicht beachtet.	31903
Beim Eingeben der Wiederholung für die geheime Antwort für Kennwortfragen wird die Groß- und Kleinschreibung nicht geprüft.	31914

Tabelle 7: Zielsystemanbindung

Gelöstes Problem	Fehler ID
<p>Fehler bei der Nutzung des Remote Connection Plugin bei deaktivierter NTLM Authentifizierung.</p> <p>i HINWEIS: Zur Behebung des Problems wurde die Konfigurationsdatei des Synchronization Editor um eine Sektion <code>remoting</code> zur Konfiguration des zu verwendenden Principal Names erweitert. Diese Änderung wirkt nur für Neuinstallationen. Bestehende Installationen werden nicht geändert.</p> <p>Für bestehende Installation: Wenn Sie von dem Problem betroffen sind, fügen Sie in die Datei <code>SynchronizationEditor.exe.config</code> folgende Einträge ein:</p> <pre><configSections> ... <section name="remoting" type="System.Configuration.NameValueSectionHandler" /> ... </configSections> <remoting> <add key="EndpointIdentity.Type" value="" /> <!-- DNS for Domain, UPN for UserPrincipalName, SPN for ServicePrincipalName --> <add key="EndpointIdentity.Value" value="" /> </remoting></pre>	31142
Beim Starten einer Synchronisation wird das korrekte Variablenset zu spät geladen.	31196
Das Synchronisationsprotokoll zeigt Objekte an, für welche die Methode Update ausgeführt wurde, obwohl die Objekte nicht geändert wurden.	31307
Der Prozess <code>DPR_Journal_Cleanup</code> blockiert unter Umständen andere Prozesse, die auf das Synchronisationsprotokoll zugreifen.	31584

Gelöstes Problem	Fehler ID
Wenn bei einer Synchronisation mehrere Objekte gelöscht werden sollen und bei einem dieser Objekte tritt ein Fehler auf, kann es passieren, dass alle Objekte nicht gelöscht werden.	31549
Fehler bei der Verarbeitung von geänderten Mitgliedschaften eines Benutzerkontos, wenn die Mitgliedschaften als ausstehend gekennzeichnet werden.	31570
Mehrere Mapping-Regeln für das identische Property führen unter Umständen zu falschen oder unvollständigen Prototyp-Objekten.	31702
Die Berechnung, welche Schematypen für das Scopehandling geladen werden müssen, nutzt den falschen Scope.	31714
Während der Synchronisation wird geprüft, ob eine Methode ausgeführt werden kann, obwohl die Methode nicht ausgeführt werden soll. Dadurch kommt es zu Fehlermeldungen.	31913
Bei der Provisionierung werden keine Änderungen in das Zielsystem geschrieben, wenn am Provisionierungsworkflow eine Quota definiert ist.	31823
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 Exchange Online-Umgebung auftreten und führt hier zu Folgefehlern. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#30269 bereitgestellt.	29152, 30269
Die Konsistenzprüfung des Windows PowerShell Konnektors erkennt nicht, wenn eine Schemaklasse keinen eindeutigen Schlüssel definiert hat.	31324
Die Seriennummer der Appliance kann nicht zur Identifizierung von PAM Appliances verwendet werden, da diese Kennung nicht eindeutig ist. Es werden Patches für Synchronisationsprojekte mit den Patch ID's VPR#31568A und VPR#31568B bereitgestellt.	31568
Inkonsistentes Verhalten bei der Behandlung von SAPComPhone.PhoneType.	29725
Fehler bei der Provisionierung von Lizenzinformationen für SAP Benutzerkonto in einer Zentralen Benutzerverwaltung.	31078
Im Manager werden unter Zielsystemabgleich: SAP R/3 Abteilungen und Personen angezeigt, die nicht aus einer SAP R/3-Umgebung stammen.	31086
Im Skript SAP_PersonAuto_Mapping_SAPUser wird für das automatische Erzeugen von Abteilungen der falsche Konfigurationsparameter verwendet und keine Datenquelle übergeben. Es wird ein neuer Konfigurationsparameter TargetSystem SAPR3 AutoCreateDepartment bereitgestellt.	31226

Gelöstes Problem**Fehler ID**

i HINWEIS: Wenn die Abteilungen durch eine SAP HCM Synchronisation eingelesen werden, sollte der Konfigurationsparameter deaktiviert sein. Anderenfalls werden die automatisch erzeugten Abteilungen als ausstehend markiert.

Fehler beim Einlesen von SAP Benutzerkonten mit führenden Leerzeichen im Namen. 31329

Zuweisungen von SAP Rollen an Benutzerkonten mit `XIsInEffect=0` werden bei jeder Synchronisation im Synchronisationsprotokoll als gelöscht angegeben. 31427

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31427 bereitgestellt.

Auf dem Formular zum Zuweisen von SAP Rollen an ein SAP Benutzerkonto werden ausstehende oder unwirksame Zuweisungen wie wirksame Zuweisungen dargestellt. 31590

Bei der Synchronisation von Standorten mit dem Schematyp `HRArea` aus einem SAP HCM System werden keine Objekte in der One Identity Manager-Datenbank aktualisiert oder neu angelegt. 31642

Der Fix korrigiert die Bildung der Schemaeigenschaft `vrtdistinguishedName`. Die Schemaeigenschaft `MOLGA` wird nicht mehr zur Bildung genutzt.

Um die Änderung anzuwenden, aktualisieren Sie im Synchronisationsprojekt das Zielsystemschemata und passen Sie das Mapping an.

Bei Generierung eines Prozesses für `SAPUserInSAPRole` wird für die SAP Rolle ein Eintrag in `QBMElementAffectedByJob` erzeugt. 31847

Für Objekte, die keine SAP Profile sind, werden Nachberechnungsaufträge `SAP-K-ProfileRestriction` für Objekte getriggert. 31886

Es ist möglich, dass bei mehreren aktivierten Preislisten in einer SAP R/3-Umgebung, die eine Schnittmenge von Lizenztypen enthalten, die Referenzauflösung am SAP Benutzerkonto scheitert, da keine eindeutige Lizenz zugeordnet werden kann. 31930

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31930 bereitgestellt.

Für kundendefinierte Zielsysteme werden auf dem Stammdatenformular die Kategorien für die Vererbung von Gruppen nicht korrekt angezeigt. 31563

Fehler beim Anlegen von kundendefinierten Zielsystemen im Manager. 31632

Fehler beim Zugriff auf das Zielsystemschemata von SharePoint Online. 31499

Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31499 bereitgestellt.

Gelöstes Problem	Fehler ID
Fehler beim Anlegen einer SharePoint Websitesammlung: Another site already exists.	31831
Beim Auslesen der SharePoint Webvorlagen wird die Schlüsseleigenschaft vr+objectPath aus Eigenschaften zusammengestellt, deren Kombination nicht eindeutig ist.	31837
<p>i HINWEIS: Die erste Synchronisation nach Einspielen dieser Version wird vorhandene SharePoint Webvorlagen (Tabelle SPSWebTemplate) als ausstehend markieren und die Einträge neu einlesen. Dies ist in der Änderung der Schlüsseleigenschaft vr+objectPath sowie des definierten Namens (DistinguishedName) begründet. Die als ausstehend markierten Webvorlagen können gelöscht werden.</p>	
Befindet sich eine SharePoint Websitesammlung im Read-Only-Modus, dann ist selbst mit dem Serverfarmkonto kein Zugriff möglich.	31904
Die Änderung des Namens eines Containers im Active Directory führt nicht zur Änderung des definierten Namens von Kindern dieses Containers im One Identity Manager.	31596, 31751
<p>i HINWEIS: Im Rahmen der Problembehebung wurde auch das Skript ADS_CreateDN zur Bildung des definierten Namens mit Maskierung korrigiert. Prüfen Sie, ob das Skript noch zu ihrer Zielsystemumgebung passt. Bei Bedarf können Sie das Skript überschreiben.</p>	
Unzureichende Fehlermeldung bei der Aktualisierung des One Identity Manager auf Version 8.1, wenn ADSSite.UID_ADSEForest leer ist.	31672
Der CN im Active Directory darf nur 64 Zeichen lang sein.	31826
Der DBQueue Prozessor Auftrag ADS-K-PersonHasADSGroup erstellt Aufträge ADS-K-ADSEContactInADSEGroup für Active Directory Benutzerkonten.	31844
Unter Umständen kann der Name der Gesamtstruktur, zu der eine Active Directory Domäne gehört, nicht ermittelt werden.	31752
Der DBQueue Prozessor Auftrag ADS-K-ADSEGroupInADSEGroup kommt unter Umständen nicht zum Ende.	31905
Fehler im Skript VI_BuildProxyAddress.	31783
Fehler im Prozess EX0_2010_EX0Mailbox_Update/Deactivate, wenn das Microsoft Exchange Postfach vor der Provisionierung nicht mehr in der Datenbank vorhanden ist.	31535
Der Anzeigename der Spalte EX0Mailbox.TotalItemSize passt nicht zum Wert.	31879
Inkonsistentes Auslesen von mehrsprachigen LDAP Attributen.	31670
Fehlerhafte Behandlung von Schemaeigenschaften, die im SCIM Schema als	31733

Gelöstes Problem	Fehler ID
returned = request gekennzeichnet sind. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31733 bereitgestellt.	
Der Prozess CSM_CSMRoot_SearchandCreate_Person_PostSync fehlt.	31864
Fehlender Scopefilter für den Schematyp PersonInLocality im Oracle E-Business Suite Konnektor. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31735 bereitgestellt.	31735
Read-Operation auf EBSSecurityGroup führt zu Fehler. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31782 bereitgestellt.	31782
Wird ein Synchronisationsprojekt mit einer kundenspezifischen Projektvorlage erstellt, werden für die Verbindungsparameter keine Variablen verwendet, sondern die feste Werte aus dem Variablenset.	31739
Der native Datenbankkonnektor unterstützt den SQL Server Datentyp Datetime2 nicht.	31741
Im nativen Datenbankkonnektor fehlt in der Methode CreateValueStore der Import Imports VI.Projector.Database.Native.	31825
Fehler beim Erstellen einer neuen Kennwortrichtlinie im Manager.	31495
Die Prozesskomponente MFRComponent fehlt.	31871
Für die beiden erweiterbaren Objektklassen racfDataset und racfResource muss das Attribut racfInstallationData in das Schema eingefügt werden.	29918
Bei der Suche nach RACF dataset-Objekten treten unter Umständen Fehler auf.	30587

Tabelle 8: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Die Beschreibung des Konfigurationsparameters QER Attestation AutoRemovalScope ESetAssignment RemoveRequestedRole ist falsch.	30481
Wenn ein Entscheidungsworkflow auf eine externe Entscheidung wartet und der Entscheidungsschritt EX für ein weiteres Attestierungsobjekt erreicht wird, dann wird der Prozess für die externe Entscheidung für alle wartenden Objekte erneut gestartet.	30965
Die Customizermethode CreateAttestations blockiert unter Umständen die Abarbeitung der DBQueue.	31016, 31370

Gelöstes Problem	Fehler ID
Das Attribut ObjectKey2 enthält in vier Privileged Account Management-spezifischen Attestierungsobjekten ein überflüssiges Zeichen ("]") in der ObjectWalker-Notation.	31547
Wenn in einem Attestierungsvorgang eine Anfrage gestellt wurde, kann es vorkommen, dass dieser Entscheidungsschritt bei Zeitüberschreitung nicht eskaliert wird.	31571
Unzureichende Primärschlüssel-Definition für die Sicht ATTVCasesOpenByPerson.	31667
AttestationRun.HistoryNumber wird nicht korrekt inkrementiert.	31373
Bei Bestellung einer Zuweisungsressource nach Referenzbenutzer wird nicht die Entscheidungsrichtlinie genutzt, die für den Referenzbenutzer verwendet wurde.	31234
Fehlende Select Berechtigung für Endbenutzer beim Attestieren.	31497
Die Konsistenzprüfung Missing table assignment to PWODecisionRule for attestation erzeugt Fehler, wenn die Präprozessorbedingung ATTESTATION deaktiviert ist.	31841
Fehler während der Aktualisierung des One Identity Manager auf Version 8.1 bei der Überprüfung kundenspezifischer Entscheidungsverfahren.	31599
Fehler beim Senden der E-Mail Benachrichtigung, wenn eine Entscheidung von einem zusätzlichen Entscheider zurückgewiesen wird.	31628
Die Methode CreateITShopOrder fehlt für Azure Active Directory Objekte.	31633
Die Spalte ITShopOrg.UID_PWODecisionMethod sollte nicht transportierbar sein, da der Wert berechnet werden muss.	31705
Fehlgeschlagene Prozessschritte für IT Shop Entscheidungen gehen nicht in den Status FROZEN .	31744
Bei Abbestellungen durch Manager ohne Genehmigungsworkflow werden keine E-Mail-Benachrichtigungen verschickt. Zur Behebung des Problems wurde die Standardmailvorlage IT Shop Bestellung - Abbestellung (IT Shop request - canceled) angepasst. Wenn Sie kundenspezifische Anpassungen vorgenommen haben, prüfen Sie den Prozess VI_ESS_PersonWantsOrg Send Mail when Unsubscribe und passen Sie diesen bei Bedarf an.	31759
In E-Mail-Benachrichtigungen für den IT Shop werden Mitglieder der zentralen Entscheidergruppe mit angezeigt.	31867
Der Prozess VI_ESS_PW0HelperPW0 approve anywhere wird nur generiert, wenn am Entscheidungsschritt eine Mailvorlage eingetragen ist.	31897

Gelöstes Problem	Fehler ID
Beim Löschen eines Eintrags aus der Tabelle BaseTree werden die Einträge aus der Tabelle PersonHasObject nicht entfernt.	31417
Migration hinterlässt BaseTreeHas*-Einträge mit XOrigin=2.	31716
Fehler beim Aufruf der Prozedur ADS_ZPersonHasObject.	31740
Falls der Nachberechnungsauftrag QER_ZAllForPersonInBaseTree durch ein Löschen eines BaseTree-Eintrag getriggert wurde, wird der notwendige Auftrag QER-K-AllForOnePerson nicht generiert.	31919
Der berechnete Risikoindex für eine Spalte wird nicht korrigiert, wenn es für die Spalte keine Risikoindex-Berechnungsvorschrift mehr gibt.	31378
Es erfolgt keine sofortige Weiterverrechnung von geänderten berechneten Risikoindezes.	31379
Fehlende Risikoindex-Berechnungsvorschriften.	31337, 31395
Bei der Bestellung von Systemrollen erkennt die Complianceprüfung der Bestellung nicht, ob durch die Unternehmensressourcen, die der Systemrolle zugewiesen sind, Complianceregel verletzt werden.	31430
Fehler im Prozess VI_QERPolicy_QERPolicyHasObject_new violation, wenn die Konfigurationsparameter für die Mailvorlagen deaktiviert sind.	31711

Tabelle 9: IT Service Management

Gelöstes Problem	Fehler ID
Ungünstige Sortierung der Ergebnislisten für Calls.	31392
Unter Umständen können beim Abrechnungslauf keinen eindeutigen Belegpositionen (Tabelle InvoiceItem) gebildet werden. Zur Behebung des Problems wurde die Bildungsregel für InvoiceItem.DisplayName angepasst. Wenn Sie kundenspezifische Bildungsregeln definiert haben, die sich auf Belegpositionen beziehen, prüfen Sie diese und passen Sie die Bildungsregeln bei Bedarf an.	31618

Siehe auch:

- [Schemaänderungen](#) auf Seite 29
- [Patches für Synchronisationsprojekte](#) auf Seite 32

Bekannte Probleme

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

Tabelle 10: Allgemein

Bekanntes Problem	Fehler ID
Fehler im Report Editor, wenn im Bericht Spalten verwendet werden, die im Report Editor als Schlüsselworte definiert sind. Workaround: Erstellen Sie Datenabfragen als SQL-Abfragen und nutzen Sie für die betroffenen Spalten Aliasnamen.	23521
Wird der Web Installer gleichzeitig in mehreren Instanzen gestartet, kann es zu Zugriffsfehlern kommen.	24198
Header-Zeilen in als CSV gespeicherten Reporten enthalten keine sprechenden Namen.	24657
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. Lösung: Laden Sie nach dem Beenden der Simulation das Objekt neu.	12753
Im Configuration Wizard können unzulässige Modulkombinationen ausgewählt werden. Dies führt erst bei Beginn der Schemainstallation zu Fehlern. Ursache: Der Configuration Wizard wurde direkt gestartet. Lösung: Verwenden Sie zur Installation der One Identity Manager Komponenten immer die autorun.exe. Damit ist sichergestellt, dass keine unzulässigen Modulkombinationen ausgewählt werden.	25315
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.	27203
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. Lösung: Markieren Sie den privaten Schlüssel beim Export und Import des Zertifikats als exportierbar.	27793
Wenn eine One Identity Manager-Datenbank im Cluster betrieben wird, wird	28373

Bekanntes Problem	Fehler ID
<p>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>	
<p>Die kundenspezifische Erweiterung von vordefinierten dynamischen Fremdschlüsseln um Referenzen auf vordefinierte Tabellen ist nicht möglich. Wenn Sie kundenspezifische dynamische Fremdschlüssel definieren, muss mindestens einer der beteiligten Partner - dynamische Fremdschlüsselspalte oder referenzierte Tabelle - ein kundenspezifisches Objekt sein.</p>	29227
<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>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 TRANSACTION within a distributed transaction.</p> <p>Lösung: Deaktivieren Sie die Option DTC_SUPPORT = PER_DB.</p>	30972
<p>Ist explizit kein Datum angegeben, wird intern das Datum 30.12.1899 verwendet. Dies ist bei Wertevergleichen zu beachten, beispielsweise bei der Verwendung in Berichten. Ausführliche Informationen zur Verwendung von Datumsangaben in Berichten finden Sie im <i>One Identity Manager Konfigurationshandbuch</i>.</p>	31322
<p>Bei der Aktualisierung der One Identity Manager-Datenbank von Version 7.0.x, 7.1.x oder 8.0.x auf die Version 8.1.1 tritt ein Fehler auf:</p> <p>Database error 41337: Cannot create memory optimized tables. To create memory optimized tables, the database must have a MEMORY_OPTIMIZED_FILEGROUP that is online and has at least one container.</p>	31981

Bekanntes Problem

Fehler ID

Ursache: Der Benutzer, mit dem die Aktualisierung der Datenbank erfolgt, besitzt nicht genügend Berechtigungen.

Lösung: Stellen Sie sicher, dass der Benutzer die SQL Server Serverrolle **dbcreator** besitzt.

Tabelle 11: Webanwendungen

Bekanntes Problem

Fehler ID

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.

26739

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.

Tabelle 12: Zielsystemanbindung

Bekanntes Problem

Fehler ID

Bei Windows PowerShell Verbindungen, welche intern Import-PSSession verwenden, kommt es zu Speicherlecks.

23795

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

- 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)

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.

Lösung: Löschen Sie die ausstehenden Zuweisungen im Zielsystemabgleich des One Identity Manager.

Der Baustein **HR_ENTRY_DATE** eines SAP HCM Systems ist standardmäßig nicht remote aufrufbar.

25401

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.

Bekanntes Problem	Fehler ID
Beim Anlegen von Microsoft Exchange Postfächern werden gegebenenfalls vorhandene sekundäre SIP-Adressen in primäre SIP-Adressen umgewandelt, sofern bisher keine primären SIP-Adressen hinterlegt waren.	27042
Der SAP Konnektor stellt keine Schemaeigenschaft bereit, um zu erkennen, ob ein Benutzer in der SAP R/3-Umgebung ein produktives Kennwort hat. Wenn diese Information im One Identity Manager zur Verfügung stehen soll, erweitern Sie das Schema und die Synchronisationskonfiguration. <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
Bei Verwendung der Bind-Methode Fast Bind in Active Directory können keine Kennwörter provisioniert werden. Die SetPassword-Methode ist somit nicht verfügbar. Der Prozessschritt AdhocProjection scheitert mit der Meldung: [System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKNOWNNAME)).	27427
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. 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.	27687
Fehler im IBM Notes Konnektor (Error getting revision of schema type ((Server))). Wahrscheinliche Ursache: Die IBM Notes-Umgebung wurde neu aufgebaut oder es wurden zahlreiche Einträge in das Domino-Verzeichnis eingefügt. Lösung: Aktualisieren Sie in der IBM Notes-Umgebung die Indexe im Domino-Verzeichnis manuell.	27126
Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer Zentralen Benutzerverwaltung. Meldung: No company is assigned. Ursache: Für das Benutzerkonto konnte keine Firmenadresse ermittelt werden. Lösung: Stellen Sie sicher, dass entweder	29253

Bekanntes Problem	Fehler ID
<ul style="list-style-type: none"> • jedem Benutzerkonto eine Firma zugeordnet ist, die im Zentralsystem existiert - ODER - • dem Zentralsystem eine Firma zugeordnet ist. 	
<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 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>	796028, 30963
<p>Bei der Einrichtung eines Synchronisationsprojektes für One Identity Safeguard wird eine Fehlermeldung angezeigt:</p>	31048

Bekanntes Problem	Fehler ID
<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>	
<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 VI.Projector.SharePoint.<Version>.Host.exe.config. 	31017
<p>Wenn eine SharePoint Websitesammlungen nur lesbar ist, kann das Serverfarmkonto die Schemaeigenschaften Owner, SecondaryContact und UserCodeEnabled nicht lesen.</p> <p>Workaround: Bei der Synchronisation werden für die Eigenschaften UID_SPSUserOwner und UID_SPSUserOwnerSecondary Leerwerte in die One Identity Manager-Datenbank geschrieben. In diesem Fall wird kein Ladefehler im Synchronisationsprotokoll aufgezeichnet.</p>	31904

Tabelle 13: Identity Management und Access Governance

Bekanntes Problem	Fehler ID
<p>Der Umzug eines Regals in einen anderen Shop und die damit verbundenen Nachberechnungsaufträge können die DBQueue blockieren.</p> <p>Lösung:</p> <p>An Regalen und Shops kann der übergeordnete IT Shop Knoten nach dem erstmaligen Speichern nicht mehr geändert werden.</p> <p>Um die Produkte eines Regals in einen anderen Shop zu verschieben</p> <ul style="list-style-type: none"> • Nutzen Sie die Aufgabe In ein anderes Regal verschieben. <ul style="list-style-type: none"> - ODER - • Weisen Sie die Produkte an ein Regal im neuen Shop zu und entfernen Sie danach die Produktzuordnungen zu dem bisherigen Regal. <p>Wenn alle Produkte verschoben wurden, kann das bisherige Regal gelöscht werden.</p>	31413

Tabelle 14: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
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 .	24626
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.	24784
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. Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am Server konfigurierte Limit.	27830
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 Uns ist derzeit nicht bekannt, ob weitere Windows Updates zu diesem Fehler führen können. 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.	30575
Unter Umständen kommt es im Report Editor zur Verwendung der falschen Sprache in den Steuerelementen von Stimulsoft.	31155
In der Manager Webanwendung kann unter Windows Server 2008 R2	31995

folgender Fehler auftreten:

```
System.Security.Cryptography.CryptographicException: Object was not found.
```

```
at System.Security.Cryptography.NCryptNative.CreatePersistedKey  
(SafeNCryptProviderHandle provider, String algorithm, String name,  
CngKeyCreationOptions options)
```

Workaround:

1. Wählen Sie im Internet Information Services (IIS)-Manager den Anwendungspool und wählen Sie den Kontextmenüeintrag **Erweiterte Einstellungen**.
2. Setzen Sie im Bereich **Prozessmodell** die Einstellung **Benutzerprofil laden** auf **True**.

Weitere Informationen finden Sie unter <https://support.microsoft.com/en-us/help/4014602>.

Schemaänderungen

Nachfolgend finden Sie eine Übersicht der Schemaänderungen von One Identity Manager Version 8.1 zu Version 8.1.1.

Modul Zielsystemsynchronisation

- Neue Spalte DPRRootObjConnectionInfo.UID_QBMServerTag zur Abbildung der Serverfunktion für Verteilung der Prozesse zur Provisionierung und Einzelobjektsynchronisation auf mehrere Jobserver.

Zielsystem Basismodul

- Verlängerung der Spalte UNSAccountB.AccountName von nvarchar(64) auf nvarchar(256).

Oracle E-Business Suite Modul

- Neue Spalten XUserInserted, XUserUpdated, XDateInserted und XDateUpdated an der Tabelle EBSUserInRespCompressed.

SAP R/3 Benutzermanagement-Modul

- Neue Spalten XUserInserted, XUserUpdated, XDateInserted und XDateUpdated an der Tabelle HelperSAPUserInSAPRole.

- Neue Spalte `SAPUserHasParameter.InheritInfo` zur Abbildung der Herkunft von Zuweisungen.
- Die Spalte `SAPUserHasParameter.ParameterValueDirect` wurde gelöscht.

Modul SAP R/3 Strukturelle Profile Add-on

- Neue Spalten `XUserInserted`, `XUserUpdated`, `XDateInserted` und `XDateUpdated` an der Tabelle `HelperSAPUserInSAPHRP`.

Privileged Account Governance Modul

- Neue Spalte `PAGReqPolicy.AllowLinkedAccountPwdAccess` als Angabe, ob Benutzer Kennwortanforderungen für ihre verknüpften Konten stellen können.
- Neue Spalte `PAGUsrGroup.UID_PAGIdentityProvider` als Verweis auf den Authentifizierungsanbieter.
- Neue Spalte `PAGIdentityProvider.DomainNames` als Liste von Domänen.
- Neue Tabelle `PAGReqPolicyHasDirAccount` zur Zuordnung mehrerer Verzeichniskonten für den Sitzungszugriff.
- Die Spalte `PAGReqPolicy.UID_PAGDirAccountSessionAccess` wurde gelöscht.
- Die Spalte `PAGUser.UID_PAGDirectory` wurde gelöscht.
- Die Spalte `PAGUsrGroup.UID_PAGDirectory` wurde gelöscht.

Identity Management Basismodul

- Neue Spalten `PersonWantsOrg.PeerGroupFactor` und `PersonWantsOrg.IsCrossFunctional` zur Unterstützung der Peer-Gruppen-Analyse für Bestellungen.
- Neue Tabelle `QERWebAuthnKey` zur Abbildung von Webauthn-Sicherheitsschlüsseln.

Modul Attestierung

- Neue Spalten `AttestationCase.PeerGroupFactor` und `AttestationCase.IsCrossFunctional` zur Unterstützung der Peer-Gruppen-Analyse für Attestierungen.
- Neue Pflichtfelddefinition für die Spalte `AttestationCase.UID_AttestationRun`.

Konfigurationsmodul

- Neue Spalten `QBMBufferTransfer.OperationType` und `QBModuleDef.CheckSumForDelta` (in Vorbereitung für zukünftige Funktionen).

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 8.1 zu Version 8.1.1. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 60.

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 32.

Tabelle 15: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Azure Active Directory Modul	Azure Active Directory Synchronization	geändert
Active Directory Modul	Active Directory Synchronization	geändert
Active Roles Modul	Synchronize Active Directory Domain via Active Roles	keine
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	keine
	Oracle E-Business Suite HR data	geändert
	Oracle E-Business Suite OIM data	keine
Microsoft Exchange Modul	Microsoft Exchange 2010 Synchronization (abgekündigt)	geändert
	Microsoft Exchange 2013/2016 Synchronization (abgekündigt)	keine
	Microsoft Exchange 2010 Synchronization (v2)	geändert
	Microsoft Exchange 2013/2016 Synchronization (v2) umbenannt in:	geändert

Modul	Synchronisationsvorlage	Art der Änderung
	Microsoft Exchange 2013/2016/2019 Synchronization (v2)	
G Suite Modul	G Suite Synchronization	keine
LDAP Modul	AD LDS Synchronization	keine
	OpenDJ Synchronization	keine
IBM Notes Modul	Lotus Domino synchronization	geändert
Exchange Online Modul	Exchange Online Synchronization (abgekündigt)	keine
	Exchange Online Synchronization (v2)	geändert
Privileged Account Governance Modul	One Identity Safeguard Synchronization	geändert
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

Nachfolgend finden Sie eine Liste aller Patches für Synchronisationsprojekte, die im One Identity Manager 8.1.1 bereitgestellt werden. 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.

WICHTIG: Manche Patches werden während der Aktualisierung des One Identity Manager automatisch angewendet. Das gilt jedoch nur, wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.1 ist.

Wenn Sie eine One Identity Manager Installation mit der Version 8.1 aktualisieren, wenden Sie diese Patches unbedingt manuell an.

Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 60.

Tabelle 16: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31456	User.CompanyName wird schreibbar	Entfernt die Zugriffsbeschränkung für die Schemaeigenschaft User.CompanyName. CompanyName ist nun schreibbar.	31456

Tabelle 17: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31419	Setzt Regelfilter an verschiedenen Synchronisationsschritten im Provisionierungsworkflow	Legt auszuschließende Regeln an den Synchronisationsschritten group, domainDNS und builtInDomain im Provisionierungsworkflow fest. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31419
VPR#31792	Korrektur von Objektfiltern	Korrigiert Objektfilter. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31792

Tabelle 18: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31165	Nutzt die lokale Serverzeit zur Revisionsfilterung	Legt neue Verbindungsparameter und Variablen für die Konfiguration der Revisionsfilterung an. Standardmäßig wird damit die lokale Serverzeit zur Revisionsfilterung genutzt.	31165
VPR#30964	Unterstützung von verknüpften	Der Patch sorgt dafür, dass auch bei LinkedRoomMailboxes die	30964

Patch ID	Patch	Beschreibung	Fehler ID
	Raumpostfächern	Schemaeigenschaften LinkedCredential, LinkedDomainController und LinkedMasterAccount an den Konnektor übergeben werden.	

Tabelle 19: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30269	Verhindert Fehler beim Laden von Einzelobjekten aufgrund gleicher Anzeigenamen	Ändert die Schemaeigenschaften vrtModBy, vrtAcceptMessagesFrom, vrtGrantSendOnBehalfOfTo, vrtRejectMessagesFrom und alle Property-Mapping-Regeln für diese Schemaeigenschaften.	30269
VPR#31166	Nutzt die lokale Serverzeit zur Revisionsfilterung	Legt neue Verbindungsparameter und Variablen für die Konfiguration der Revisionsfilterung an. Standardmäßig wird damit die lokale Serverzeit zur Revisionsfilterung genutzt.	31166

Tabelle 20: Patches für die Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31735	Scopefilter für Schematyp PersonInLocality	Erzeugt einen Scopefilter für den Schematyp PersonInLocality . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31735
VPR#31782	Definition von Sicherheitsgruppen	Korrigiert die Definition von Sicherheitsgruppen. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31782
VPR#31794	Korrektur von Scopefiltern	Korrigiert Scopefilter. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31794

Tabelle 21: Patches für IBM Notes

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31420	Setzt Regelfilter an	Legt auszuschließende Regeln an	31420

Patch ID	Patch	Beschreibung	Fehler ID
	verschiedenen Synchronisationsschritten im Provisionierungsworkflow	den Synchronisationsschritten Certifier und Policy im Provisionierungsworkflow fest. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	

Tabelle 22: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31459	Mapping der Schemaeigenschaft AllowLinkedAccount PasswordAccess	Fügt in das Mapping AccessRequestPolicy eine Property-Mapping-Regel für die Schemaeigenschaft AllowLinkedAccountPasswordAccess ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31459
VPR#31568A	Ersetzt Appliance serial als Appliancenummerierung durch eine kundendefinierte Kennung (Teil 1)	Ersetzt Appliance serial als eindeutige Kennung des Basisobjekts durch eine kundendefinierte Kennung und wendet diese Änderung in der Konfiguration der Synchronisation an. Voraussetzung für Patch Ersetzt Appliance serial als Appliancenummerierung durch eine kundendefinierte Kennung (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31568
VPR#31568B	Ersetzt Appliance serial als Appliancenummerierung durch eine kundendefinierte Kennung (Teil 2)	Ersetzt Appliance serial als eindeutige Kennung des Basisobjekts durch eine kundendefinierte Kennung und wendet diese Änderung in der Konfiguration der Synchronisation an. Abhängig von Patch Ersetzt Appliance serial als Appliancenummerierung durch eine kundendefinierte Kennung (Teil 1) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31568

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31569	Verbesserungen für One Identity Safeguard Cluster	<p>Fügt Verbindungsparameter und Variablen für die Verbindung von One Identity Safeguard Clustern hinzu.</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p> <p>Wenn Sie One Identity Safeguard Cluster verwenden, sollte nach dem Anwenden des Patches der Systemverbindungsassistent erneut ausgeführt werden, um die Appliances des Clusters zu ermitteln.</p>	31569
VPR#31664A	Änderungen für Zugriffsanforderungsrichtlinien für den Sitzungszugriff (Teil 1)	<p>Eine Zugriffsanforderungsrichtlinie kann mehrere Verzeichniskonten für Sitzungszugriffe erhalten.</p> <p>Voraussetzung für Patch Änderungen für Zugriffsanforderungsrichtlinien für den Sitzungszugriff (Teil 2).</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	31664
VPR#31664B	Änderungen für Zugriffsanforderungsrichtlinien für den Sitzungszugriff (Teil 2)	<p>Eine Zugriffsanforderungsrichtlinie kann mehrere Verzeichniskonten für Sitzungszugriffe erhalten.</p> <p>Abhängig von Patch Änderungen für Zugriffsanforderungsrichtlinien für den Sitzungszugriff (Teil 1).</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	31664
VPR#31703	Alternative Regel für die Mappings Directory und IdentityProvider	<p>Fügt alternative Regeln für die Mappings Directory und IdentityProvider ein.</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	31703
VPR#31775A	Änderung von Referenzen für	<p>Entfernt für Benutzer und Benutzergruppen die Referenz zum</p>	31775

Patch ID	Patch	Beschreibung	Fehler ID
	Benutzer und Benutzergruppen (Teil 1)	Verzeichnis und fügt für Benutzergruppen eine Referenz zum Authentifizierungsanbieter ein. Voraussetzung für Patch Änderung von Referenzen für Benutzer und Benutzergruppen (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
VPR#31775B	Änderung von Referenzen für Benutzer und Benutzergruppen (Teil 2)	Entfernt für Benutzer und Benutzergruppen die Referenz zum Verzeichnis und fügt für Benutzergruppen eine Referenz zum Authentifizierungsanbieter ein. Abhängig von Patch Änderung von Referenzen für Benutzer und Benutzergruppen (Teil 1) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31775

Tabelle 23: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31412	Definiert auszuschließende Regeln für die Provisionierung	Definiert auszuschließende Property-Mapping-Regeln im Synchronisationsschritt user des Provisionierungsworkflows. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31412
VPR#31427	Legt eine Schemaklasse für den Schematyp SAPUserInSAPRole an	Legt die Schemaklasse AssignmentsInEffect für den Schematyp SAPUserInSAPRole mit dem Filter XIsInEffect <> '0' an. Die Schemaklasse wird in den Mappings userInRole und userInCUARole genutzt.	31427
VPR#31796	Korrektur von Objektfiltern	Korrigiert Objektfilter. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31796
VPR#31930	Änderung des	Korrigiert den Referenzscope für den	31930

Patch ID	Patch	Beschreibung	Fehler ID
	Referenzscope für den Schematyp SAPLicence	Schematyp SAPLicence in der One Identity Manager Verbindung.	

Tabelle 24: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31499	Schemaeigenschaft Site.NewUrl entfernen	Entfernt die Schemaeigenschaft NewUrl aus dem Mapping Site. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31499

Tabelle 25: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31733	Schemaeigenschaften mit Rückgabety request	Aktualisiert das Konnektorschema, um Schemaeigenschaften mit dem Rückgabety request zu behandeln. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31733
VPR#31756	Scope für Zugriffstoken	Erstellt einen Scope für Zugriffstoken als neuen Verbindungsparameter.	31756

Patches in One Identity Manager Version 8.1

Tabelle 26: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext DPR .	
	Meilenstein 8.1.1	Meilenstein für den Kontext One Identity Manager .	

Tabelle 27: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext Azure Active Directory .	

Tabelle 28: 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 Schemaklasse 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 Schemaklasse ADSSite (all) (Teil 2)	Ändert den Fremdschlüssel für ADSSite von ADSDomain zu ADSForest. Abhängig von Patch Korrektur der Schemaklasse ADSSite (all) (Teil 1) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	29306
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 8.1.1	Meilenstein für den Kontext Active Directory .	

Tabelle 29: 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 8.1.1	Meilenstein für den Kontext Active Roles .	

Tabelle 30: 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 PersonManager. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	29265
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	Ändert das Serialisierungsformat an den Schematypen. Das Zielsystemschemata wird neu geladen. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31011
Meilenstein 8.1.1		Meilenstein für den Kontext Oracle E-Business Suite .	

Tabelle 31: 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 8.1.1	Meilenstein für den Kontext Microsoft Exchange.	

Tabelle 32: 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 8.1.1	Meilenstein für den Kontext Exchange Online.	

Tabelle 33: Patches für G Suite

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext G Suite .	

Tabelle 34: Patches für LDAP

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext LDAP .	

Tabelle 35: 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 8.1.1	Meilenstein für den Kontext IBM Notes .	

Tabelle 36: 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

Patch ID	Patch	Beschreibung	Fehler ID
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 8.1.1	Meilenstein für den Kontext SAP R/3 .	

Tabelle 37: 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
	Meilenstein 8.1.1	Meilenstein für den Kontext SAP R/3 Strukturelle Profile Add-on .	

Tabelle 38: Patches für SAP R/3 BI Analyseberechtigungen

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext SAP R/3 Analyseberechtigungen Add-on .	

Tabelle 39: 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 8.1.1	Meilenstein für den Kontext SAP R/3 .	

Tabelle 40: Patches für SharePoint

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext SharePoint .	

Tabelle 41: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30729	Korrigieren der Eigenschaft Pflichtfeld des SharePoint OnlineUser.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 8.1.1	Meilenstein für den Kontext SharePoint Online .	

Tabelle 42: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30497	Ermöglicht die Konfiguration des lokalen Caches	Fügt eine Variable hinzu, über welche die Nutzung des lokalen Caches deaktiviert werden kann. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	30497
VPR#31250	Korrekturen in den Skripten virtueller Schemaeigenschaften	Ergänzt einen NULL-Wert-Test in den Get-Skripten von virtuellen Schemaeigenschaften. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31250
	Meilenstein 8.1.1	Meilenstein für den Kontext SCIM .	

Tabelle 43: Patches für die Universal Cloud Interface-Schnittstelle (im Modul Cloud Systems Management)

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext Universal Cloud Interface .	

Tabelle 44: Patches für Unix

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext Unix .	

Tabelle 45: Patches für den One Identity Manager Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	Meilenstein für den Kontext Datenbank .	

Tabelle 46: Patches für den CSV-Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.1.1	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.

- Google ReCAPTCHA Version 1 wird nicht mehr unterstützt.
- Die Prozesskomponente SvnComponent wurde entfernt.
- Der Konfigurationsparameter **Common | MailNotification | DefaultCultureFormat** wurde gelöscht.

Bei Bedarf muss die kundenspezifische Verwendung angepasst werden. Die Sprache für die Wertformatierung wird über die Person ermittelt.

- Folgende Skripte wurden entfernt, da deren Funktion obsolet oder nicht mehr sichergestellt war:
 - VI_Del_ADSSAccountInADSGroup
 - VI_GetDNSHostNameOfHardware
 - VI_GetDomainsOfForest
 - VI_GetServerFromADSContainer
 - VI_Make_Ressource
 - VID_CreateDialogLogin

- VI_Discard_Mapping
- VI_Export_Mapping
- VI_GenerateCheckList
- VI_GenerateCheckListAll

Für künftige One Identity Manager Versionen werden folgende Funktionen 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.
- Der Systembenutzer **viITShop** wird zukünftig nicht mehr unterstützt und gelöscht.
Verwenden Sie die rollenbasierte Anmeldung über entsprechende Anwendungsrollen.
- Das Skript VI_BuildPwdMessage wird zukünftig nicht mehr unterstützt und gelöscht.
Zum Versenden der E-Mail-Benachrichtigungen mit Anmeldeinformationen werden Mailvorlagen verwendet. Die Mailvorlagen sind in den Konfigurationsparametern **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** und **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** eingetragen.

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
	i 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>i 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 2019 • 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 2019 • 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>

- NTP - Client
- Mono 5.14 oder höher
- Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
 - 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 2019 • 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 47: Unterstützte Datensysteme

Konnektor	Unterstützte Datensysteme
Konnektor für Trennzeichen getrennte Textdateien	Beliebige durch Trennzeichen getrennte Textdateien.
Konnektor für relationale Datenbanken	<p>Beliebige relationale Datenbanken, die ADO.NET unterstützen.</p> <p>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.</p>
Generischer LDAP	Beliebiger LDAP Version 3 konformer Verzeichnisserver. Der LDAP

Konnektor	Unterstützte Datenysteme
Konnektor	<p>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.</p> <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	<p>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.</p>
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 2019 mit kumulativem Update 1 • Microsoft Exchange Hybrid-Umgebungen
SharePoint Konnektor	<ul style="list-style-type: none"> • SharePoint 2010 • SharePoint 2013 • SharePoint 2016 • SharePoint 2019
SAP R/3 Konnektor	<ul style="list-style-type: none"> • SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2 und 7.50 • SAP ECC 5.0 und 6.0 • SAP S/4HANA On-Premise-Edition
Unix Konnektor	<p>Unterstützt werden die gängigsten Unix und Linux Derivate. Weitere Informationen finden Sie in den Spezifikationen für Authentication Services.</p>

Konnektor	Unterstützte Datenysteme
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 • 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, 7.3.1
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, 2.6, 2.7

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 8.1.1 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 54.

Hinweise zur Aktualisierung des One Identity Manager

- Stellen Sie vor der Aktualisierung der One Identity Manager-Datenbank auf die Version 8.1.1 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 8.1.1 funktioniert nur, wenn das Service Pack 7.0.3 installiert ist. Zusätzlich müssen die Dateien VI.Update.d11 und JobService.d11 installiert sein.

Fordern Sie die Dateien VI.Update.d11 und JobService.d11 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 8.1.1 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. Stellen Sie sicher, dass der Benutzer, mit dem die Installation oder Aktualisierung der One Identity Manager-Datenbank ausgeführt wird, die SQL Server Serverrolle **dbcreator** besitzt.

- Während der Aktualisierung einer One Identity Manager-Datenbank der Versionen 7.0, 7.1 oder 8.0 auf die Version 8.1.1 werden diverse Spalten zu physischen Pflichtfeldern, die bereits semantisch als Pflichtfelder definiert waren.

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 oder einer neuen One Identity Manager History Database mit der Version 8.1.1 sowie der Aktualisierung einer One Identity Manager-Datenbank oder One Identity Manager History Database von den Versionen 7.0.x, 7.1.x oder 8.0.x auf die Version 8.1.1 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 bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter <https://support.oneidentity.com/identity-manager/> erreichbar.

- 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 8.1.1

! **WICHTIG:** Beachten Sie die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 54.

Um eine bestehende One Identity Manager Installation auf die Version 8.1.1 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.

1 | **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.

1 | **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 oder Version 8.1.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.

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

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

- HINWEIS:** Wenn Sie bei der Aktualisierung von den Versionen 7.0.x, 7.1.x oder 8.0.x auf die Version 8.1.1 auf das abgestufte Berechtigungskonzept wechseln möchten, verwenden Sie einen Installationsbenutzer mit den Berechtigungen für dieses Rechtekonzept. Ausführliche Informationen zu den Berechtigungen finden Sie im *One Identity Manager Installationshandbuch*.

Wenn Sie bei der Aktualisierung von der Version 8.1.x auf die Version 8.1.1 zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter <https://support.oneidentity.com/identity-manager/> erreichbar.

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 oder Version 8.1.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 8.1.1 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 60.

Um einen Anwendungsserver auf die Version 8.1.1 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 8.1.1 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 einen API Server auf die Version 8.1.1 zu aktualisieren

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

Um das Web Portal für Betriebsunterstützung auf die Version 8.1.1 zu aktualisieren

- (von Version 8.1.x) Nach der Aktualisierung des API Servers kompilieren Sie die HTML-Anwendung **Operations Support Portal**. Ausführliche Anweisungen finden Sie im *One Identity Manager Installationshandbuch*.
- (von Version 8.0.x)
 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 8.1.1 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** die Patches aus, die angewendet werden sollen. Mehrfachauswahl ist möglich.
Im Bereich **Details - Installationszusammenfassung** werden die 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. Prüfen Sie anhand des Patchprotokolls, ob kundenspezifische Anpassungen nachbearbeitet werden müssen.
7. Falls erforderlich, überarbeiten Sie die kundenspezifischen Anpassungen in der Synchronisationskonfiguration.
8. Führen Sie eine Konsistenzprüfung durch.
9. Simulieren Sie die Synchronisation.
10. Aktivieren Sie das Synchronisationsprojekt.
11. 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 31
- [Patches für Synchronisationsprojekte](#) auf Seite 32

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 2019.0001.0021.0100 für alle Module und die Anwendungsversion 8.1 2019-01-21-108 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.