

One Identity Manager 8.1.4

Versionshinweise

19. Oktober 2020, 09:33 Uhr

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 8.1.4 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 8.1.3 aufgeführt.

One Identity Manager 8.1.4 ist ein Patch Release mit neuen Funktionen und verbessertem Verhalten. Siehe [Neue Funktionen](#) auf Seite 2 und [Verbesserungen](#) auf Seite 3.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.1.3 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

Die aktuellsten Versionen der Produktdokumentation finden Sie unter [One Identity Manager Dokumentation](#).

Über One Identity Manager 8.1.4

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.

Starling Cloud Join

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

Neue Funktionen

Neue Funktionen in One Identity Manager 8.1.4.

Basisfunktionen

- Neue Konfigurationsmöglichkeit zur Erkennung und Mailbenachrichtigung, wenn der One Identity Manager Service keine Anfragen mehr ausführt.

Über den neuen Konfigurationsparameter **Common | MailNotification | NotifyAboutRequestStall** legen Sie fest, ob eine Benachrichtigung erfolgen soll. Der Konfigurationsparameter ist im Standard deaktiviert. Die weitere Konfiguration erfolgt über den neuen Zeitplan **Benachrichtigung, wenn ein Jobserver keine Prozesse mehr verarbeitet**. Der Zeitplan muss passend zum Konfigurationsparameter **Common | Jobservice | LoadedJobsTimeOut** konfiguriert sein.

Zielsystemanbindung

- Unterstützung von One Identity Active Roles Version 7.3.3, Version 7.4.1 und Version 7.4.3.

Identity Management und Access Governance

- Unterstützung der OAuth 2.0 Authentifizierung für Exchange Online Postfächer bei Attestierungen per E-Mail und bei Entscheidungen per E-Mail.

Die Funktion nutzt den Exchange Web Service (EWS). Registrieren Sie im Microsoft Azure Management Portal in ihrem Azure Active Directory Mandanten eine Anwendung, beispielsweise **One Identity Manager Approval by Mail**. Die Anwendungs-ID, die bei der Registrierung erzeugt wurde, tragen Sie in die neuen Konfigurationsparameter **QER | Attestation | MailApproval | AppId** und **QER | ITShop | MailApproval | AppId** ein.

Ausführliche Informationen, wie Sie die Anwendung registrieren, finden Sie unter <https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth#register-your-application>.

Siehe auch:

- [Verbesserungen](#) auf Seite 3
- [Gelöste Probleme](#) auf Seite 5
- [Schemaänderungen](#) auf Seite 27
- [Patches für Synchronisationsprojekte](#) auf Seite 29

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die im One Identity Manager 8.1.4 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Der Umfang der SQL Protokollierung wurde erweitert, wenn SQL Anweisungen wiederholt werden müssen.	33268
Ausnahmen, die für die Wiederholungsversuche von SQL Anweisungen verantwortlich sind, werden protokolliert.	33462
Verbesserte Prüfung von mehrteiligen Namensbestandteilen in Kennwortrichtlinien, wenn die Option Namensbestandteile unzulässig aktiviert ist.	33245

Verbesserung	Fehler ID
Verbesserte Performance für verschiedene SQL Funktionen.	33066, 33080
Verbesserte Performance bei der Übernahme in die History Database.	33438, 33439
Verkürzung der Abarbeitungszeit in der DBQueue aufgrund optimierter Einstellung von automatisch generierten Berechnungsaufträgen.	33454
Die datenbankinterne Kommunikation zur Koordination der Verarbeitung von DBQueue Prozessor Aufträgen wurde optimiert. Das datenbankinterne Nachrichtenaufkommen (MessageBroker) wurde reduziert. Des Weiteren werden, bei gleicher Sortierung, nun Nachberechnungsaufträge mit wenigen Nachfolgeaufträgen gegenüber von Nachberechnungsaufträge mit vielen Nachfolgeaufträgen priorisiert, um die Gesamtanzahl gleichzeitig wartender Aufträge zu reduzieren.	33453

Tabelle 2: Allgemein Webanwendungen

Verbesserung	Fehler ID
Verbesserte Performance bei der Ermittlung der verwendeten Leistungspositionen für Bestellungen im Web Portal.	33256
Im Web Portal werden nun leere Datumsfelder mit einem Beispielwert angezeigt, sodass man das erwartete Datumsformat schnell erkennen kann.	33493
Die folgenden Javascript-Bibliotheken wurden aktualisiert: <ul style="list-style-type: none"> • Bootstrap: Version 3.4.1 • AngularJS: Version 1.7.9 	254323

Tabelle 3: Zielsystemanbindung

Verbesserung	Fehler ID
Auf dem Stammdatenformular für Zielsystemtypen im Manager wird die Spalte AdditionalSystemTypes (Alternative Konnektoren) angezeigt.	33366
Der SCIM Konnektor unterstützt Cookies des SCIM Providers in REST-Anfragen.	33051
Der SAP Konnektor unterstützt das Setzen von produktiven Kennwörtern bei Anmeldung über Secure Network Communications (SNC) mit Single-Sign-On.	33455, 33461
Korrektur der Referenz von SAP Firmen auf SAP Benutzerkonten zur Unterstützung von SAP S/4HANA 2.0. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32347 bereitgestellt.	32347

Verbesserung	Fehler ID
Verbesserte Anzeige der Testergebnisse, wenn im Systemverbindungsassistenten für Cloud-Anwendungen die Verbindung zu den SCIM-Endpunkten getestet wird.	33232
Verbesserte Protokollierung für den nativen Datenbankkonnektor bei der Anbindung einer Datenbank über den generischen ADO.NET Provider.	33079

Siehe auch:

- [Schemaänderungen](#) auf Seite 27
- [Patches für Synchronisationsprojekte](#) auf Seite 29

Gelöste Probleme

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

Tabelle 4: Allgemein

Gelöstes Problem	Fehler ID
<p>Fehlende Berechtigungen für administrative Benutzer zum Ermitteln von Informationen zur Ausführung von Datenbankschedules durch den SQL Server Agent aus der Tabelle <code>dbo.sysjobhistory</code>.</p> <p>Um die Berechtigungen zu vergeben</p> <ul style="list-style-type: none"> • Führen Sie folgende SQL-Anweisung in einem geeigneten Programm aus. <pre>Use msdb Go GRANT SELECT ON OBJECT::syschedules TO [OneIMRole_<DatabaseName>] go</pre>	33179
Obwohl die Datenbank nicht verschlüsselt ist, kann für kundenspezifische Konfigurationsparameter die Option verschlüsselt aktiviert werden.	33089
Beim Kopieren von Berechtigungsgruppen, tritt im Kopierassistent ein Fehler auf: Copy started. Copy failed with following error: [810025] DialogColumnGroupRight: Write permission denied for value "CanEdit".	33253
Die Konsistenzprüfung QBMRelation invalid (QBM_FTRelationValidationInfo) hat eine von Schema Extension angelegte Tabellenbeziehung von einer Datenbanksicht vom Typ View (beispielsweise Department) zu einer Tabelle vom Typ Basistabelle (beispielsweise BaseTree) als ungültig ausgegeben.	33130

Gelöstes Problem	Fehler ID
Ist das Tabellenskript Skript (OnDiscarded) komplett leer, wird das Tabellenskript Skript (OnDiscarding) nicht ausgeführt. Das Problem tritt nicht auf, wenn im Tabellenskript Skript (OnDiscarded) etwas enthalten ist, beispielsweise eine Kommentarzeile.	33252
<p>Ein abonniertes Bericht mit der Option Einfacher Listenbericht enthält keine Kopfzeile.</p> <p>Ab One Identity Manager Version 8.0 werden einfache Listenberichte nicht mehr über die Prozessfunktion Export der Prozesskomponente ReportComponent erstellt, sondern über die Prozessfunktion CSVExportSingle der Prozesskomponente ScriptComponent erzeugt. Bei dieser Umstellung wurde die Kopfzeile (Parameter Header) nicht ergänzt</p> <p>Das Skript RPS_ParseReportDefinitionXML wurde erweitert. Die Prozesse RPS_RPSSubscription_Send_Report, RPS_RPSSubscriptionCC_Send_Report_to_CC, RPS_RPSSubscription_Store_Report und RPS_RPSSubscriptionCC_Store_Report_for_CC wurden angepasst.</p>	33261
<p>Wartungsaufträge zum erneuten Aufbauen der Tabellenindexe (QBM-K-CommonReIndexTable) laufen potentiell sehr lange oder schlagen aufgrund der Laufzeit fehl, werden wiederholt und verschwinden deshalb nie aus der DBQueue.</p> <p>Die Aktualisierung der Statistiken wurde aus dem Auftrag QBM-K-CommonReIndexTable entfernt und in einen neuen Auftrag QBM-K-UpdateStatistics ausgelagert. Der Auftrag aktualisiert die Statistiken nicht mehr für jede Tabelle einzeln, sondern führt die gespeicherte Prozedur sp_updatestats aus. Damit erfolgt Aktualisierung wesentlich performanter.</p>	33172
<p>Bei paralleler Ausführung von Änderungen, die einen Eintrag in der Tabelle DialogProcess anlegen würden, kommt es potentiell zum Fehler: VI.DB.DatabaseException: Database error 2627: Violation of PRIMARY KEY constraint 'PK_DialogPr__2B66FD776487EDFB'. Cannot insert duplicate key in object 'dbo.DialogProcess'.</p>	33188
<p>Die Anmeldung am Launchpad mit den Authentifizierungsmodulen Active Directory Benutzerkonto (rollenbasiert) und Active Directory Benutzerkonto (manuelle Eingabe/rollenbasiert) ist in Version 8.1.x nicht möglich.</p>	33318
<p>Es kann zu massivem Vorkommen der Aufträge zu Neuberechnung der Entscheider (QER-K-ShoppingRackPW0He1perPW0-Cfg) in der DBQueue kommen, die andere Aufträge blockieren.</p>	33083
<p>Im Schemaeditor fehlt sporadisch für Tabellen der Tabreiter ViewAddons. Man muss erst mehrmals hin und her klicken, damit der Tabreiter angezeigt wird.</p>	33171
<p>Aufträge, die sehr lange in der DBQueue verweilen und immer wieder</p>	33338

Gelöstes Problem	Fehler ID
wiederholt werden, verschwinden irgendwann ohne Berechnung aus der DBQueue.	
<p>Beim Vergeben der abgestuften Berechtigungen für Objekte, die nicht zum dbo-Schema gehören, tritt ein Fehler auf: Cannot find the object 'MyTable', because it does not exist or you do not have permission.</p> <p>Beim dem Vergeben der abgestuften Berechtigungen wird jetzt geprüft, ob die Objekte zum dbo-Schema gehören. Schemafremde Objekte erhalten keine abgestuften Berechtigungen.</p>	33164
<p>Bei der Installation der History Database in einer verwalteten Instanz in Azure SQL-Datenbank tritt ein Fehler auf: Database error 41906: Statement ,BEGIN DISTRIBUTED TRANSACTION' is not supported in SQL Database Managed Instance.</p>	33307
<p>Relativ kleine Werte im Konfigurationsparameter Common ProcessState PackageSizeHDB werden beim Übertragen der Daten in die History Database nicht beachtet.</p>	33363
<p>Für Systembenutzer können gleichzeitig die Optionen Dienstkonto und Nur Leserechte gesetzt werden.</p> <p>Das Verhalten wurde geändert. Die Optionen können jetzt nicht mehr gleichzeitig verwendet werden.</p>	33195
<p>Fehler bei Erstellen eines kundenspezifischen Formulars mit der Formulardefinition VI_Common_Assignment_Overview (FrmCommonAssignmentOverview).</p>	33325
<p>Im Dialog für die erweiterten Eigenschaften eines Objektes werden auf dem Tabreiter Rechte die Bearbeitungsrechte für die Rechtegruppen nicht richtig angezeigt.</p>	33464
<p>Beim Speichern von zusätzlichen Sichtdefinitionen (QBViewAddOn) kann es zu Fehlern kommen, wenn in der Datenbank bereits sehr umfangreiche Daten in Sichtdefinitionen gespeichert wurden, sodass die Daten im SQL Server ausgelagert werden (Spalte Blob (extern) ist gesetzt).</p>	33409
<p>Beim Herunterfahren der Slots für den DBQueue Prozessor aufgrund des Erreichens der maximalen Lebensdauer laut Konfigurationsparameter QBM DBQueue KeepAlive kann es vermehrt zu Meldungen im Systemprotokoll der Art kommen:</p> <pre>#LDS#Dead slot resetted, number={0}, type = {1}, Task = {2}, code = {3}. 4 DeadTest <none> 2 </pre>	33460
<p>Die Spalte Baumbene (TreeLevel) wird, in den von der Tabelle BaseTree abgeleiteten Sichten, beim Einfügen neuer Objekte, wie beispielsweise Anwendungsrollen, nicht gefüllt.</p>	33489
<p>Berichte mit historischen Daten zeigen inaktive Zuweisungen als noch zugewiesen. Im Bericht ist die Spalte Zugewiesen bis leer.</p>	33393

Tabelle 5: Allgemein Webanwendungen

Gelöstes Problem	Fehler ID
Unter bestimmten Umständen kommt es im Web Portal beim Öffnen von umfangreichen Berichten zu einem Fehler.	32896
Im Web Portal wird der Text für die Begründung einer Entscheidung zu einer offenen Bestellung mit dem Text einer vorherigen, abgeschlossenen Entscheidung vorausgefüllt.	33152
Die Anmeldung am Kennwortrücksetzungsportal über den Link in der E-Mail für die Anmeldung funktioniert nicht.	32885
Fehlerhafte Übersetzung in der Tabelle DialogMultiLanguage führt bei der Verwendung der Kennwortrichtlinien im Kennwortrücksetzungsportal zum Fehler.	33278
Beim Kompilieren eines Webprojekts kommt es zu folgendem Fehler: An error occurred while generating source code in <Webprojekt>. Error while generating code for configuration key: TableSearch_Person Object reference not set to an instance of an object.	33346
Im Web Portal funktionieren Links im Detailbereich eines Objekts nicht.	33210
Unter bestimmten Umständen kommt es beim Aktualisieren der Vorschau im Web Designer zu einem Fehler.	33180
Im Web Portal auf der Seite Delegierungen löscht die Schaltfläche Alle meine Delegierungen löschen nur die Delegierungen der ersten Seite.	33186
Im Web Portal werden Gruppenmitgliedschaften, die indirekt durch untergeordnete Gruppen zugewiesen wurden, nicht mehr angezeigt.	33216
Wenn der Genehmiger eines Attestierungsvorgangs im Web Portal eine negative Entscheidung trifft und die negative Entscheidung zur Abbestellung eines Produkts führt, dann wird in der Bestellhistorie zur entsprechenden Bestellung fälschlicherweise der Empfänger als Entscheider angezeigt.	33255
Im Web Designer können Gültigkeitsdaten für alle Produkte im Warenkorb gesetzt werden. Produkte, für die bereits ein Gültigkeitsdatum/-zeitraum gesetzt ist, werden dabei nicht berücksichtigt. Beim Bearbeiten des Einkaufswagens im Web Portal gibt es nun jeweils für Gültig von und Gültig bis die Optionen Bereits vorhandene Datumsangaben ersetzen , mit denen man für alle Produkte im Einkaufswagen das eingestellte Gültigkeitsdatum verwendet, unabhängig davon, ob bereits individuell ein Datum am Produkt gesetzt wurde.	33322
Im Web Portal ist es beim Verlängern der Gültigkeit eines Produkts möglich, die Gültigkeit über das erlaubte Maß hinaus zu setzen.	33410
Wenn ein Entscheider im Web Portal für eine Bestellung zuerst ein falsches und anschließend ein korrektes Gültigkeitsdatum setzt, kommt es zum	33343

Gelöstes Problem	Fehler ID
Fehler.	
Beim Bearbeiten eines neu erstellten Abonnements im Web Portal wird das Abonnement unter bestimmten Umständen fälschlicherweise gelöscht.	33468
Die Tabreiter der Monitorseite des Web Portal enthalten keine Informationen.	33457
Unter bestimmten Umständen findet die Suche im Web Portal nicht das gesuchte Objekt.	33387
Unter bestimmten Umständen stürzt der Anwendungsserver beim Start des Indizierungsvorgangs ab.	33174
Beim Anzeigen von Diagrammen im Web Portal kommt es beim Abwählen aller anzuzeigenden Diagramme mithilfe des Diagramm-Filters zum Fehler.	33501
Beim Kompilieren im API Designer kommt es zum Fehler, wenn man relative Pfade in der .config-Datei verwendet.	33505
Wenn das Web Portal direkt mit der Datenbank verbunden ist, kommt es zu starken Verzögerungen und langen Ladezeiten.	33470
Wenn man die Seite <WebPortal>/ae.axd öffnet, um die Erreichbarkeit des Web Portals zu prüfen, wird eine neue Sitzung erstellt.	33389
Wenn man im Web Portal ein Produkt bestellt und diese Bestellung anschließend über die Bestellhistorie storniert, kommt es zum Fehler.	33146

Tabelle 6: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Mitgliedschaften, die im One Identity Manager eingefügt aber noch nicht provisioniert wurden, werden durch eine gleichzeitig laufende Synchronisation als ausstehend markiert.	33144
Beim Importieren eines Synchronisationsprojekts mit dem Database Transporter wird die Importoption Einstellungen für die Startkonfiguration nicht ändern nicht beachtet, wenn sie aktiviert ist. Änderungen an der Startkonfiguration und an Variablen werden in der Zieldatenbank überschrieben.	33153
Wenn im One Identity Manager eine Mitgliedschaft hinzugefügt wird, die zuvor im Zielsystemabgleich gelöscht wurde, dann wird diese Änderung nicht ins Zielsystem provisioniert.	33201
In bestimmten Situationen werden bei der Provisionierung von Objekteigenschaften die Mitgliedschaften der betroffenen Objekte im Zielsystem komplett mit den Mitgliedschaften ersetzt, die in One Identity Manager vorhanden sind, obwohl die Einzelprovisionierung von Mitgliedschaften konfiguriert ist. Das führt dazu, dass direkt im Zielsystem vorgenommene Änderungen überschrieben werden.	33205

Gelöstes Problem	Fehler ID
<p>Der Fehler tritt auf, wenn von einer M:N Eigenschaft abhängige andere Schemaeigenschaften provisioniert werden sollen. Aufgrund der Abhängigkeit werden auch die Mitgliedschaften provisioniert. Wenn es zu diesem Zeitpunkt jedoch keine Mitgliedschaftsoperation in der Tabelle DPRMembershipAction gibt, wird die komplette Mitgliederliste übertragen.</p>	
<p>Wenn in einem Variablenset Skriptvariablen verwendet werden, dann werden in das Synchronisationsprotokoll für die Skriptvariablen nicht die Werte des verwendeten Variablensets geschrieben, sondern die Werte des Standardvariablensets. Variablen mit festen Werten werden korrekt protokolliert.</p> <p>Bei der Synchronisation werden die korrekten Variablenwerte verwendet. Lediglich die Protokollierung der Skriptvariablen ist falsch.</p>	33229
<p>Das Transportpaket für ein Synchronisationsprojekt lässt sich unter folgenden Bedingungen nicht importieren:</p> <ul style="list-style-type: none"> • Das Synchronisationsprojekt ist in der Zieldatenbank bereits vorhanden. • Das Quellprojekt enthält nicht alle im Zielprojekt referenzierten Objekte. 	33257
<p>Es kommt zu einer FK-Verletzung.</p> <p>Beim Transport von Synchronisationsprojekten wird die Eigenschaft von Tabellenrelationen Bei Übermengenbehandlung ignorieren nicht beachtet. Der Database Transporter versucht referenzierte Objekte zu löschen, die in der Zieldatenbank vorhanden sind, im Transportpaket jedoch fehlen.</p>	
<p>Fehler beim Provisionieren neuer Mitgliedschaften, die in der One Identity Manager-Datenbank wieder gelöscht wurden (<code>XOrigin='0'</code>), bevor der Provisionierungsprozess für die Neuanlage verarbeitet wurde.</p>	33267
<p>Wenn für verschiedene kundendefinierte Zielsystemtypen die Einzelprovisionierung von Mitgliedschaften konfiguriert ist, werden bei jeder Änderung einer Mitgliedschaft mehrere Einträge in der Tabelle DPRMemberShipAction erzeugt. Es entsteht ein Eintrag für jeden Zielsystemtyp, für den der Merge-Modus für die Tabelle UNSAccountBINUNSGroupB aktiviert ist. Erwartet wird jedoch nur ein Eintrag für den Zielsystemtyp, in dem die Mitgliedschaft geändert wurde.</p>	33365
<p>Wenn im Synchronization Editor die Wartung des Synchronisationspuffers manuell gestartet wird, erscheint eine Fehlermeldung mit dem Hinweis, dass der Prozess DPR_MaintainDataStore nicht generiert werden kann.</p>	33391
<p>Fehler beim Öffnen eines Synchronisationsprojekts im Synchronization Editor mit einem Benutzer, der nur Leserechte hat: <code>Write permission denied for values: EditedBy, EditedSince.</code></p>	33394

Gelöstes Problem**Fehler ID**

Der Synchronisation Editor schreibt beim Öffnen eines Synchronisationsprojekts den aktuellen Benutzer und die Uhrzeit an das Projekt und speichert es in die One Identity Manager-Datenbank (Tabelle DPRShe11). Diese Funktion soll Datenverlust verhindern, indem es andere Benutzer, welche das selbe Synchronisationsprojekt öffnen, informiert, dass dieses bereits in Bearbeitung ist. Der Synchronisation Editor prüft jedoch nicht, ob der angemeldete Benutzer Schreibrechte auf diese Tabelle hat.

Im Synchronisationsprotokoll ist ein Objekt als geändert protokolliert. Es ist jedoch für keine Objekteigenschaft eine Änderung aufgezeichnet, obwohl das Synchronisationsprotokoll so konfiguriert ist, dass geänderte Eigenschaften und Werte protokolliert werden.

33402

Wenn die geänderte Objekteigenschaft einen geheimen Wert enthält oder der Wert **NULL** ist, wird diese Änderung nicht im Synchronisationsprotokoll aufgezeichnet.

Lösung: Die Protokollierung wurde geändert. Geheime Werte werden als **<hidden>** protokolliert und ein NULL-Wert wird mit **<null>** protokolliert.

Property-Mapping-Regeln mit eingeschränkter Mappingrichtung und dem Zusatz **Einschränkungen bei der Neuanlage ignorieren** funktionieren bei der Synchronisation ins Zielsystem nicht.

33437

Bei der Synchronisation mit dem nativen Datenbankkonnektor können einige Objekte aus dem Zielsystem nicht geladen werden. Es erscheint die Fehlermeldung: No suitable key property found for reloading!

33258

Der Wert der Schlüsseleigenschaft entspricht dem Standardwert des jeweiligen Datentyps. Wenn beispielsweise der Primärschlüssel den Datentyp Integer und den Wert **0** hat, dann erkennt der native Datenbankkonnektor das als Leerwert und verwendet diesen Wert nicht, um das Objekt zu selektieren.

SQL Fehler bei der Synchronisation mit dem nativen Datenbankkonnektor, wenn in der Verbindungskonfiguration zur externen Datenbank eine musterbasierte Strategie für die Ausführung von Datenoperationen definiert ist und ein referenzierter Spaltenname Leerzeichen enthält.

33274

Lösung: Der native Datenbankkonnektor nutzt den ScriptSafeIdentifier. Spaltennamen mit Sonderzeichen können nun referenziert werden, wenn die Sonderzeichen durch Unterstrich ersetzt werden. Sonderzeichen sind alle Zeichen außer Buchstaben, Ziffern und Unterstrich.

Beispiel: Insert Into MyTab([ColPK],[Col Spaces]) Values(%ColPK%, %Col_Spaces%)

Bei der Synchronisation mit dem nativen Datenbankkonnektor können neue Objekte nicht im Zielsystem gespeichert werden. Es erscheint die Fehlermeldung: Unable to create the primary key where clause for system object ...

33370

Gelöstes Problem	Fehler ID
Fehler beim Einrichten eines Synchronisationsprojekts für eine CData ADO.NET Provider Datenbank mit dem nativen Datenbankkonnektor. Der Fehler tritt nur auf, wenn die Treiberversion 2020 verwendet wird.	33484
Die Synchronisationsvorlagen für Oracle E-Business Suite und SCIM legen den Referenzscope mit deutschem Anzeigenamen an. Es werden Patches für Synchronisationsprojekte mit den Patch IDs VPR#33259_SCIM, VPR#33259_EBS bereitgestellt.	33259
Fehler beim Schreiben von Objekten mit dem SCIM Konnektor, wenn die Zielsystem-Umgebung Anfragen mit der HTTP Header Option Expect: 100-continue" nicht unterstützt. Die Anfrage wird mit HTTP Status 417 "Expectation failed beantwortet. Der SCIM Konnektor wertet das als Fehler und beendet den Vorgang.	33220
Wenn im SCIM-Konnektorschema eine komplexe Schemaeigenschaft definiert ist, kann es vorkommen, dass der SCIM Konnektor deren untergeordnete Schemaeigenschaften nicht zurückgibt. Entsprechend fehlen diese Schemaeigenschaften im Synchronization Editor, beispielsweise in der Schemaansicht des Zielsystems im Mappingeditor.	33233
Wenn eine komplexe Schemaeigenschaft im SCIM-Schema als Pflichteigenschaft gekennzeichnet ist, scheitert die Provisionierung, weil eine Pflichteigenschaft nicht gemappt ist.	33241
Fehler bei der Synchronisation mit dem SCIM Konnektor, wenn für ein Objekt die Schemaeigenschaft id ein Pflichtfeld ist. Im One Identity Manager ist die Schemaeigenschaft id entsprechend der SCIM Spezifikation als nur lesbar gekennzeichnet. Wenn durch eine kundenspezifische Schemaerweiterung die Schemaeigenschaft id für ein Objekt als schreibbar angelegt wird, dann wird diese Eigenschaft im erweiterten Schema des One Identity Manager dennoch als nur lesbar abgebildet. Im PUT Request dieses Objekts wird die id damit nicht übertragen. Der SCIM Provider antwortet mit der Fehlermeldung Missing required attribute [id].	33336
Fehler beim Provisionieren von Mitgliedschaften, wenn der SCIM Provider die PATCH-Methode unterstützt. Wenn die virtuelle Schemaeigenschaft members~vrtIDandType geschrieben wird, welche die Einzelwerte auf die untergeordneten Schemaeigenschaften members~type und members~value verteilen soll, kommt es zum Fehler im SCIM Konnektor.	33459
Der SCIM Konnektor gibt nicht korrekt an, wenn ein SCIM Provider keine Filter unterstützt. In den Synchronisationsprojekten können Systemfilter definiert werden. Diese sind jedoch nicht wirksam, wenn der SCIM Konnektor auf das Zielsystem zugreift.	33483
Im One Identity Manager kann man Active Directory-Objekte anlegen, die	33032

Gelöstes Problem	Fehler ID
sich nur in diakritischen Zeichen (beispielsweise ê, ü) unterscheiden. Im Active Directory ist das nicht zulässig. Es entsteht ein Prozessschritt mit dem Status Frozen , weil dieses Objekt im Active Directory schon existiert.	
Das Home- und das Profilverzeichnis eines Active Directory Benutzerkontos werden sofort gelöscht, wenn das Benutzerkonto zum Löschen markiert wird.	33202, 33092
Öffnet man im Manager das Stammdatenformular für mehrere über Mehrfachauswahl gewählte Active Directory Gruppen und öffnet auf dem Formular die Auswahlliste Kontomanager , dann reagiert das Programm nicht mehr.	33177
Wenn ein Active Directory Schema in einem bestehenden Synchronisationsprojekt nach Erstellung durch eine Projektvorlage aktualisiert wird, fehlen in allen Schematypen, die nicht bereits im gespeicherten Schema vorhanden waren, die Inhalte in den berechneten Schemaeigenschaften AuxiliaryClasses, ContainerClasses, AllSuperClasses und AllSearchClasses.	33246
Bei Zuweisung eines Active Directory Computers zur einem Gerät wird kein Nachberechnungsauftrag ADS-K-ADSMachineInADSGroup eingestellt. Damit werden Gruppen, die über das Gerät vererbt werden, nicht an den Computer zugewiesen.	33420
Auf dem Stammdatenform für Active Directory Benutzerkonten ist das Steuerelement für die Eigenschaft Einwahl erlaubt immer aktiv, auch wenn Benutzer nur Leserechte für die Eigenschaft haben. Eine Änderung des Wertes ist zwar möglich, auch beim Speichern kommt kein Fehler. Allerdings wird die Änderung nicht gespeichert.	33463
Bei Laden von Active Directory Objekten für die Provisionierung arbeitet die Typprüfung zu stringent.	33138
Fehler bei Zuweisen einer Person zu einem Active Directory Benutzerkonto, wenn das Benutzerkonto ein verknüpftes Microsoft Exchange Postfach ohne verbundenes Benutzerkonto (EX0Mailbox.UID_ADSAccountLinkedMaster) besitzt.	33317
Die Kontaktdaten eines Azure Active Directory Benutzerkontos mit einem Exchange Online Postfach können nur gepflegt werden, wenn das Postfach vom Empfängertyp Benutzerpostfach (UserMailbox) ist.	33191
Fehler bei der Synchronisation von Azure Active Directory Gruppen, die an Azure Active Directory Administratorrollen zugewiesen sind. Zur Behebung des Fehlers wurde im Mapping DirectoryRole ein Mitgliederfilter definiert, der nur Benutzerkonten einschließt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33399 bereitgestellt.	33399

Gelöstes Problem	Fehler ID
<p>Die Exchange Online Synchronisation scheitert bei Aktualisierung von Telefonnummern von Exchange Online E-Mail Benutzern mit zugehörigem Azure Active Directory Benutzerkonto vom Typ Guest.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33476 bereitgestellt.</p>	33476
<p>Die Spalten 03EDynDL.Notes, 03EMailContact.Notes, 03EMailUser.Notes und 03EUnifiedGroup.Notes sind zu kurz.</p>	33392
<p>Unzureichende Fehlermeldung beim Parsen eines definierten Namens (DistinguishedName) eines LDAP Objektes. Das fehlerhafte Objekt wird nicht ausgegeben.</p>	33310
<p>Fehler beim Einlesen von SAP Benutzerkonten, wenn in einem SAP Mandant Anreden definiert sind, die in verschiedenen Sprachen identisch sind. Die Referenzen zur Anrede können nicht aufgelöst werden.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33147 bereitgestellt.</p>	33147, 33447
<p>Öffnet man im Synchronization Editor den Zielsystembrowser für eine angebundene SAP R/3-Umgebung und wählt in einer beliebigen Ergebnisliste ein Einzelobjekt, so werden keine Objekteigenschaften angezeigt.</p>	33168
<p>Bei der Erweiterung des SAP Schemas mit einer Schemaerweiterungsdatei wird kein Fehler erkannt, wenn in einer Funktionsdefinition das Attribut OutStructure zwar den korrekten Datentyp BAPIRET2 hat, jedoch der Name der SAP-Struktur nicht RETURN, RETURNØ oder BAPIRET2 ist.</p>	33200
<p>Wenn in der Schematypdefinition einer Schemaerweiterungsdatei für den Aufruf der Objektliste und für den Aufruf des Einzelobjekts unterschiedliche Tabellen genutzt werden, dann greift der SAP R/3 Konnektor beim Aufbau des Schemas und beim Lesen der Objekte nur auf die Tabelle zu, die im Attribut ListObjectsDefinition angegeben ist.</p>	33218
<p>SAP Rollen werden bei der Synchronisation als gelöscht oder ausstehend gekennzeichnet, wenn dieselbe Rolle sowohl als Einzelrolle als auch über eine Sammelrolle vererbt wird. Das Verhalten tritt auf, wenn der Konfigurationsparameter TargetSystem SAPR3 KeepRedundantProfiles aktiviert ist.</p>	33244
<p>Auf dem Überblicksformular für eine SAP Rolle wird nicht angezeigt, welchen IT Shop Regalen diese Rolle zugewiesen ist.</p>	33361
<p>Bei der Synchronisation in eine SAP R/3-Umgebung summieren sich die Fehlermeldungen im Synchronisationsprotokoll, wenn im Synchronisationsprojekt Bei Fehler fortsetzen konfiguriert ist.</p>	33416
<p>Wenn die Änderung an der Anrede eines SAP Benutzerkontos provisioniert wird, schlägt der Prüfschritt Check Properties SAP fehl. Das Verhalten tritt</p>	33423

Gelöstes Problem	Fehler ID
<p>auf, wenn der SAP R/3 Konnektor bei der Provisionierung mit einer anderen Anmeldesprache auf das Zielsystem zugreift, als der Sprache, aus welcher die gesetzte Anrede ursprünglich stammt.</p> <p>Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33423 bereitgestellt.</p>	
Wenn das zentrale Kennwort einer Person im One Identity Manager geändert wird, dann wird das SAP Benutzerkonto dieser Person gesperrt.	33450
Kann eine Verbindung zur IBM Notes-Umgebung nicht sofort hergestellt werden, weil bereits ein anderer Prozess eine Verbindung zu diesem System nutzt, wird auf die Beendigung dieses Prozesses gewartet und es wird eine Warnung ausgegeben, wenn auch im Wartezeitintervall keine Verbindung aufgebaut werden konnte. Für die Ausgabe der Warnung wird auf eine Eigenschaft des Domino-Servers zugegriffen, der nicht erreicht werden kann. Es kommt zum Fehler: "Domino server not connected."	33283
Wenn der Konfigurationsparameter TargetSystem NDO MailBoxAnonymPre deaktiviert ist, werden Notes Benutzerkonten nicht anonymisiert, wenn sie gesperrt werden. Werden diese Benutzerkonten später entsperrt, wird der Prozess NDO_NDOUserInGroup_ChangeNamesOn(un)Lock ausgeführt, obwohl der vollständige Name der Benutzerkonten nicht geändert wurde.	33330

Tabelle 7: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
<p>Der Prozess QER_Person_Publish_CentralPassword läuft unter Umständen für das selbe Objekt mehrmals parallel. Das kann passieren, wenn es mehrere Kennwortänderungen innerhalb eines Verarbeitungsintervalls des One Identity Manager Service für diesen Jobserver gab. In diesem Fall sind mehrere dieser Prozesse gleichzeitig in der Queue und werden zeitgleich verarbeitet.</p> <p>Um die korrekte Abarbeitungsreihenfolge zu erzwingen, wurde im Prozess QER_Person_Publish_CentralPassword der Prozessschritt Publish password to all accounts von der Prozessfunktion ScriptExec auf die Prozessfunktion ScriptExecExclusive geändert.</p>	33132
<p>Fehler bei Berechnung der Attestierer in der Prozedur ATT_PAttestationHelperFill.</p> <p>Obwohl für einen Entscheidungsschritt kein regulärer Attestierer ermittelt werden kann, wird der Attestierungsvorgang nicht an die Fallback-Entscheider übergeben. Der Entscheidungsschritt wird automatisch abgelehnt. Das Verhalten tritt auf, wenn der Konfigurationsparameter QER Attestation PersonToAttestNoDecide aktiviert ist und eine zu attestierende Person als einziger Attestierer ermittelt wird.</p>	33151
Durch den Entscheidungsworkflow Attestierung von Zuweisungen zu	33187

Systemberechtigungen (inklusive Active Directory) werden die falschen Entscheider ermittelt. Für Active Directory Gruppen werden die Zielsystemverantwortlichen ermittelt und für alle anderen Systemberechtigungen werden die Produkteigner ermittelt. Es soll jedoch genau umgekehrt sein.

Bei einer errechneten Entscheidung werden nicht die am Entscheidungsschritt definierten Begründungstexte (**Begründung Genehmigung** oder **Begründung Ablehnung**) am Attestierungsvorgang eingetragen. Stattdessen wird der Standard-Begründungstext "Entscheidung nach Verfahren CD wurde vom System vorgenommen ..." verwendet. Die SQL-Prozedur ATT_ZAttestationMakeDecisionCD wurde korrigiert.

33344

Wenn Attestierungsvorgänge für dauerhaft deaktivierte Personen automatisch geschlossen werden, bleibt die Begründung für die Entscheidung unverändert. Sie enthält damit nicht die Begründung für die Schließung.

33345

Der Trigger ATT_TUPerson wurde geändert. Am geschlossenen Attestierungsvorgang wird nun folgender Begründungstext eingetragen: "Entscheidung wurde vom System vorgenommen. Attestierungsvorgang geschlossen, da die Person dauerhaft deaktiviert wurde."

Wenn für einen Entscheidungsschritt in der Tabelle AttestationHelper mehrere Einträge mit derselben Person existieren, beispielsweise als Attestierer und als zentrale Entscheidergruppe, dann kann es vorkommen, dass bei einer Delegation der Entscheidung das Mitglied der zentralen Entscheidergruppe seine Verantwortung delegiert und die Person immer noch als regulärer Attestierer den Attestierungsvorgang entscheiden kann.

33360

Wenn nach Abschluss eines Genehmigungsverfahrens Einträge in der Hilfstabelle für Bestellvorgänge (Tabelle PWOHelperPWO) gelöscht werden, können Deadlocks entstehen. Sowohl in die Jobqueue als auch in die DBQueue werden Löschaufträge für dieselbe abgeschlossene Bestellung eingestellt. Diese behindern sich.

33327

Der Menüeintrag **Azure Active Directory > Basisdaten > Zielsystemtypen** (AzureAD.BasicInformation.DPRNameSpace) zeigt den Zielsystemtyp **Exchange Online** nicht mit an.

33368

Der Auftrag ATT-K-AttestationHelper-Cfg ist übermäßig häufig mehrfach in der DBQueue vorhanden. Durch eine Migration auf One Identity Manager 8.1.2 wird dieser Effekt zusätzlich verstärkt. Dadurch entsteht eine hohe Last auf der DBQueue, sodass andere Aufträge nicht zeitnah verarbeitet werden.

33082

Durch Änderungen in Personenzuordnungen und durch die Aktualisierung des One Identity Manager wird pro Person der Auftrag QER-K-AllForPersonInBaseTree in die DBQueue eingestellt. Dieser führt pro Person eine Neuberechnung des Auftrags ATT-K-AttestationHelper-Cfg aus und stellt diesen Auftrag für jeden offenen Attestierungsvorgang ein.

Gelöstes Problem	Fehler ID
Die Prozeduren ATT_PAttestationHelperFillAll und QBM_ZRecalculate wurden so geändert, dass keine mehrfachen Aufträge ATT-K-AttestationHelper-Cfg für denselben Attestierungsvorgang in die DBQueue eingestellt werden.	
Mitunter werden zugewiesene Bestellungen nach Umzug des Produkts in einen anderen Shop abgebrochen, obwohl die Person auch in dem neuen Shop Kunde ist.	33137
Entscheidungsschritte werden bei Überschreiten des Timeout nicht automatisch entschieden, solange für ein Mitglied der zentralen Entscheidergruppe das Timeout noch nicht erreicht ist.	33436
Beim Öffnen des Berichtes Übersicht mit Geschäftsrollen und Benutzerkonten (inklusive Historie) stürzt das Frontend zum Beispiel Manager oder Report Editor ab, wenn die geöffnete Person sehr viele Änderungsaufzeichnungen hat.	33502

Tabelle 8: IT Service Management

Gelöstes Problem	Fehler ID
Wenn der Konfigurationsparameter QBM WorkingHours IgnoreWeekend aktiviert ist, werden die Standardarbeitsstunden aus Ländern und Bundesländern nicht beachtet.	33414

Siehe auch:

- [Schemaänderungen](#) auf Seite 27
- [Patches für Synchronisationsprojekte](#) auf Seite 29

Bekannte Probleme

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

Tabelle 9: Allgemein

Bekanntes Problem	Fehler ID
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

Bekanntes Problem	Fehler ID
Header-Zeilen in als CSV gespeicherten Berichten 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
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.	29227
Fehler beim Auslösen von Ereignissen auf eine View, welche keine UID-Spalte als Primärschlüssel besitzt. 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. Die Definition einer View, die als Primärschlüssel den XObjectKey verwendet, ist nicht zulässig und wird an sehr vielen Stellen zu weiteren Fehlern führen. Zur Überprüfung des Schemas wird eine Konsistenzprüfung Table of type U or R with wrong PK definition bereitgestellt.	29535

Bekanntes Problem	Fehler ID
Die Standardeinstellungen der <code>globallog.config</code> gehen davon aus, dass die Rechte zum Schreiben in <code>%localappdata%</code> vorhanden sind. Hat eine EXE nicht die richtigen Berechtigungen, kann man durch Änderung der Variable <code>logBaseDir</code> in der <code>globallog.config</code> oder durch Einführung einer speziellen Log-Konfiguration in der <code>*.exe.config</code> oder <code>Web.config</code> das Protokoll in ein Verzeichnis schreiben lassen, für das Rechte bestehen.	30048
Wenn die One Identity Manager-Datenbank in einem SQL-Cluster (High Availability Group) installiert ist und die Option <code>DTC_SUPPORT = PER_DB</code> gesetzt ist, erfolgt die Replikation zwischen den Servern mittels Distributed Transaction. Fehler, falls dabei ein Save Transaction ausgeführt wird: <code>Cannot use SAVE TRANSACTION within a distributed transaction.</code> Lösung: Deaktivieren Sie die Option <code>DTC_SUPPORT = PER_DB</code> .	30972
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> .	31322
Bei der Installation der Datenbank unter SQL Server 2019 tritt ein Fehler auf: <code>QBM_PDBQueueProcess_Main unlimited is only allowed as an agent job</code> Lösung: <ul style="list-style-type: none"> Das kumulative Update 2 für SQL Server 2019 wird nicht unterstützt. Weitere Informationen finden Sie unter https://support.oneidentity.com/kb/315001 .	32814

Tabelle 10: 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. Lösung: Ändern Sie auf dem Elternordner der Webanwendung (standardmäßig <code>C:\inetpub\wwwroot</code>) die Berechtigungen für den Benutzer und wenden Sie diese Änderung an. Nehmen Sie anschließend diese Änderung wieder zurück.	26739
Die Bestelleigenschaften eines Produktes werden bei der Verlängerung oder Abbestellung im Web Portal nicht aus der ursprünglichen Bestellung in den Warenkorb übernommen. Ursache: Bestelleigenschaften können in unterschiedlichen, kundenspezifischen Spalten gespeichert werden.	32364

Bekanntes Problem	Fehler ID
Lösung: Erstellen Sie eine Bildungsregel für die (kundenspezifische) Spalte an der Tabelle ShoppingCartItem, in der die Bestelleigenschaft bei der Bestellung gespeichert wird. Diese Bildungsregel muss die Bestelleigenschaften für die verknüpfte Bestellung aus der identischen (kundenspezifischen) Spalte an der Tabelle PersonWantsOrg auslesen.	
Es ist nicht möglich mithilfe des Web Designer in der Kopfzeile neben dem Firmennamen/-logo einen Link im Web Portal zu platzieren.	32830
Es ist möglich im Web Portal einen Bericht zu abonnieren, ohne dabei einen Zeitplan auszuwählen.	32938
Workarounds: <ul style="list-style-type: none"> • Erstellen Sie eine Erweiterung auf das entsprechende Formular, mit der unter der Auswahlliste ein Hinweistext angezeigt wird, der auf das Problem hinweist. • Legen Sie einen Standard-Zeitplan für abonnierbare Berichte fest. • Ändern Sie im Web Designer den Konfigurationsschlüssel Filter für abonnierbare Berichte (VI_Reporting_Subscription_FilterRPSSubscription) und setzen Sie den Wert von Minimale Anzahl Zeichen des Zeitplans (UID_DialogSchedule) auf 1. 	

Tabelle 11: Zielsystemanbindung

Bekanntes Problem	Fehler ID
Bei Windows PowerShell Verbindungen, welche intern Import-PSSession verwenden, kommt es zu Speicherlecks.	23795
Der Baustein HR_ENTRY_DATE eines SAP HCM Systems ist standardmäßig nicht remote aufrufbar. 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.	25401
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
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
Der SAP Konnektor stellt keine Schemaeigenschaft bereit, um zu erkennen, ob ein Benutzer in der SAP R/3-Umgebung ein produktives Kennwort hat.	27359

Bekanntes Problem**Fehler ID**

Wenn diese Information im One Identity Manager zur Verfügung stehen soll, erweitern Sie das Schema und die Synchronisationskonfiguration.

- 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.

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.

27687

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.

Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer Zentralen Benutzerverwaltung.

29253

Meldung: No company is assigned.

Ursache: Für das Benutzerkonto konnte keine Firmenadresse ermittelt werden.

Lösung: Stellen Sie sicher, dass entweder

- jedem Benutzerkonto eine Firma zugeordnet ist, die im Zentralsystem existiert
- ODER -
- dem Zentralsystem eine Firma zugeordnet ist.

Bei der Synchronisation von SAP R/3 Personalplanungsdaten, die erst zukünftig wirksam werden, werden einige Daten nicht eingelesen.

29556

Ursache: Die Funktion BAPI_EMPLOYEE_GETDATA wird immer mit dem aktuellen Tagesdatum ausgeführt. Damit werden Änderungen taggenau beachtet.

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.

Fehler bei der Synchronisation einer OpenDJ-Umgebung, wenn ein Kennwort mit einer öffnenden geschweiften Klammer beginnt.

29620

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.

Lösung: LDAP Server können so konfiguriert werden, dass ein bereits

Bekanntes Problem	Fehler ID
<p>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. 	
<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 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. - 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
<p>Wenn Datumsfelder in einer SAP R/3-Umgebung Werte enthalten, die kein</p>	32149

gültiges Datums- oder Uhrzeitformat repräsentieren, kann der SAP Konnektor diese Werte nicht lesen, da die Typkonvertierung scheitert.

Lösung: Bereinigen Sie die fehlerhaften Daten.

Workaround: Die Typkonvertierung kann deaktiviert werden. Voraussetzung dafür ist, dass auf dem Synchronisationsserver der SAP .Net Connector for .NET 4.0 on x64, mindestens Version 3.0.15.0 installiert ist.

WICHTIG: Da mit diesem Workaround die Datumsprüfung komplett umgangen wird, sollte er nur genutzt werden, wenn keine andere Lösung umsetzbar ist.

Um die Typkonvertierung zu deaktivieren

- Fügen Sie folgende Einstellungen in die Datei `StdioProcessor.exe.config` ein.
 - In die vorhandene Sektion `<configSections>`:


```
<sectionGroup name="SAP.Middleware.Connector">
  <section name="GeneralSettings"
    type="SAP.Middleware.Connector.RfcGeneralConfiguration,
    sapnco, Version=3.0.0.42, Culture=neutral,
    PublicKeyToken=50436dca5c7f7d23" />
</sectionGroup>
```
 - Eine neue Sektion:


```
<SAP.Middleware.Connector>
  <GeneralSettings anyDateTimeValueAllowed="true" />
</SAP.Middleware.Connector>
```

Die in der Prozesskomponente `PowershellComponentNet4` im Parameter `OutputFile` zu erzeugende Datei enthält keine Fehlermeldungen.

32945

Ursache:

In der Datei (Parameter `OutputFile`) werden keine Meldungen gesammelt. Die Datei dient als Exportdatei der in der Pipeline zurückgelieferten Objekte.

Lösung:

Die Ausgabe von Meldungen im Skript kann mittels `*>` Operator in eine im Skript festgelegte Datei erfolgen.

Beispiel:

```
Write-Warning "Ich bin eine Meldung" *> "meldungen.txt"
```

Weiterhin werden Meldungen, die Mittels `Write-Warning` generiert werden, ebenfalls in die Protokolldatei des One Identity Manager Service geschrieben. Möchte man einen Abbruch mit Fehler im Skript erzwingen, so sollte man eine `Exception` werfen. Diese Meldung erscheint dann in der

Bekanntes Problem**Fehler ID**

Protokolldatei des One Identity Manager Service.

Der G Suite Konnektor kann die Nutzerdaten von Google Applikationen vor dem Löschen eines Benutzerkontos nicht erfolgreich auf ein anderes G Suite Benutzerkonto übertragen. Der Transfer scheitert an den Nutzerdaten der Applikation Rocket.

33104

Workaround: Hinterlegen Sie in den erweiterten Einstellungen der Systemverbindung zur G Suite ein Applikationstransfer XML. In diesem XML-Dokument schränken Sie die Liste der zu übertragenden Nutzerdaten ein. Führen Sie nur die Google Applikationen auf, deren Nutzerdaten Sie weiterhin benötigen. Ein Beispiel-XML sehen Sie beim Bearbeiten des Applikationstransfer XML im Systemverbindungsassistenten.

Um die Liste der zu übertragenden Nutzerdaten einzuschränken

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Der Systemverbindungsassistent wird gestartet.
4. Auf der Startseite des Systemverbindungsassistenten aktivieren Sie **Erweiterte Einstellungen anzeigen**.
5. Auf der Seite **Erweiterte Einstellungen** erfassen Sie im Eingabefeld **Applikationstransfer XML** das XML-Dokument.
6. Speichern Sie die Änderungen.

Enthalten Zielsystemdaten nachgestellte Leerzeichen so gehen diese bei der Synchronisation in den One Identity Manager verloren. Jede weitere Synchronisation erkennt Datenänderungen und schreibt die betroffenen Werte immer wieder oder legt neue Objekte an, wenn diese Eigenschaften Teil der Object-Matching-Regel ist.

33448

Lösung:

Nachgestellte Leerzeichen sollten bereits im Zielsystem vermieden werden.

Tabelle 12: Identity Management und Access Governance**Bekanntes Problem****Fehler ID**

Der Umzug eines Regals in einen anderen Shop und die damit verbundenen Nachberechnungsaufträge können die DBQueue blockieren.

31413

Lösung:

An Regalen und Shops kann der übergeordnete IT Shop Knoten nach dem erstmaligen Speichern nicht mehr geändert werden.

Um die Produkte eines Regals in einen anderen Shop zu verschieben

- Nutzen Sie die Aufgabe **In ein anderes Regal verschieben**.

Bekanntes Problem	Fehler ID
<p>- ODER -</p> <ul style="list-style-type: none"> 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>	
<p>Bei der Genehmigung einer Bestellung mit Selbstbedienung wird das Ereignis Granted für den Entscheidungsschritt nicht ausgelöst. In kundenspezifischen Prozessen kann stattdessen das Ereignis OrderGranted genutzt werden.</p>	31997

Tabelle 13: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
<p>Unter SharePoint 2010 kann es zu einem Fehler bei der Synchronisation von SharePoint Websites kommen. Die Methode SPWeb.FirstUniqueRoleDefinitionWeb() löst eine ArgumentException aus. Weitere Informationen finden Sie unter https://support.microsoft.com/de-de/kb/2863929.</p>	24626
<p>Die Installation des One Identity Manager Service mit Server Installer auf einem Windows Server funktioniert nicht, wenn die Einstellung File and Printer Sharing am Server deaktiviert ist. Auf einem Domänen-Controller ist diese Einstellung aus Sicherheitsgründen deaktiviert.</p>	24784
<p>Beim Verbinden mit einer Oracle Database kommt es sporadisch zu einem der folgenden Fehler: TNS-12516, TNS-12519 oder ORA-12520. Erneute Verbindungsversuche sind jedoch meist erfolgreich.</p> <p>Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am Server konfigurierte Limit.</p>	27830
<p>In einem mehrseitigen Synchronisationsprotokoll kann nicht mit der Maus und mit den Pfeiltasten navigiert werden.</p> <p>Ursache: Die StimulReport.Net-Komponente der Firma Stimulsoft behandelt den Bericht als eine Seite.</p>	29051
<p>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.</p>	762534, 762548, 29607
<p>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:</p> <ul style="list-style-type: none"> Windows Server 2016 : KB4462928 Windows Server 2012 R2 : KB4462926, KB4462921 Windows Server 2008 R2 : KB4462926 	30575

Bekanntes Problem**Fehler ID**

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.

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 folgender Fehler auftreten: 31995

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>.

Bei der Anbindung eines externen Webservices über den Webservice-Integrationsassistenten stellt der Webservice die Daten über eine WSDL-Datei bereit. Mittels des WSDL-Tools von Microsoft werden diese Daten in Visual Basic .NET Code umgewandelt. Wenn im so generierten Code Standard-Datentypen überschrieben werden (beispielsweise wenn nochmals der Datentyp boolean definiert wird), kann das im One Identity Manager zu verschiedenen Problemen führen. 31998

In bestimmten Active Directory/Microsoft Exchange-Topologien schlägt das Cmdlet Set-Mailbox mit folgendem Fehler fehl: 33026

Error on proxy command 'Set-Mailbox...'

The operation couldn't be performed because object '...' couldn't be found on '...'.

Weitere Informationen finden Sie unter <https://support.microsoft.com/en-us/help/4295103>.

Mögliche Workarounds:

- Verbinden Sie sich mit dem Microsoft Exchange Server, auf dem sich das Benutzerpostfach befindet. Verwenden Sie dazu einen kundenspezifischen Prozess. Nutzen Sie den Parameter `OverrideVariables` (Prozesskomponente `ProjectorComponent`) um den Server (Variable `CP_ExchangeServerFqdn`) zu überschreiben.
- Da das Problem nur bei einigen Schemaeigenschaften auftritt, sollten Sie in Erwägung ziehen, diese Schemaeigenschaften im Synchronisierungsprojekt gegen Schreiboperationen zu schützen. Sie können die Schemaeigenschaften in einem kundenspezifischen Prozess unter Verwendung der Prozesskomponente `PowershellComponentNet4` über einen benutzerdefinierten Windows PowerShell-Aufruf setzen lassen.

Schemaänderungen

Nachfolgend finden Sie eine Übersicht der Schemaänderungen von One Identity Manager Version 8.1.3 zu Version 8.1.4.

Konfigurationsmodul

- Neue Spalte `QBMDBQueueTaskPerf.CountChildTasks`.

Identity Management Basismodul

- Neue Spalten `AccProduct.IsDeactivatedByPreProcessor` und `AccProduct.PreProcessorCondition`.
- Neue Spalten `PWODecisionMethod.IsDeactivatedByPreProcessor` und `PWODecisionMethod.PreProcessorCondition`.

Exchange Online Modul

- Verlängerung der Spalten `O3EDynDL.Notes`, `O3EMailContact.Notes`, `O3EMailUser.Notes` und `O3EUnifiedGroup.Notes` auf `nvarchar(1024)`.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 8.1.3 zu Version 8.1.4. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere

Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 63.

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 29.

Tabelle 14: 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	keine
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	geändert
	Oracle E-Business Suite HR data	geändert
	Oracle E-Business Suite OIM data	geändert
Microsoft Exchange Modul	Microsoft Exchange 2010 Synchronization (abgekündigt)	keine
	Microsoft Exchange 2013/2016 Synchronization (abgekündigt)	keine
	Microsoft Exchange 2010 Synchronization (v2)	keine
	Microsoft Exchange 2013/2016/2019 Synchronization (v2)	keine
G Suite Modul	G Suite Synchronization	keine
LDAP Modul	AD LDS Synchronization	keine
	OpenDJ Synchronization	keine
IBM Notes Modul	Lotus Domino synchronization	keine

Modul	Synchronisationsvorlage	Art der Änderung
Exchange Online Modul	Exchange Online Synchronization (abgekündigt)	keine
	Exchange Online Synchronization (v2)	keine
Privileged Account Governance Modul	One Identity Safeguard Synchronization	keine
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 8.1.4 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. Manche Patches werden während der Aktualisierung des One Identity Manager automatisch angewendet.

Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 63.

Tabelle 15: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33399	Filtert die Mitglieder von Administratorrollen	Fügt einen Mitgliederfilter für Benutzerkonten in die Property-Mapping-Regel vrtMember_Members im Mapping DirectoryRole ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	33399

Tabelle 16: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33259_EBS	Anzeigename des Referenzscopes	Korrigiert den Anzeigenamen des Referenzscopes.	33259

Tabelle 17: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33476	Korrektur der Mappingrichtung für Mobiltelefon und Telefon (geschäftlich) für Gastbenutzer	Korrigiert die Mappingrichtung für die Schemaeigenschaften MobilePhone und Phone im Mapping MailUser .	33476

Tabelle 18: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32347	Korrektur der Referenz von SAP Firmen auf SAP Benutzerkonten	Korrigiert die Referenzauflösung zu SAP Firmen im Mapping user zur Unterstützung von SAP S/4HANA 2.0.	32347
VPR#33147	Korrektur des Imports von SAP Anreden	Änderungen im Mapping title , um den Import von SAP Anreden zu korrigieren sowie die Referenzauflösung zu den SAP Benutzerkonten. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	33147
VPR#33423	Korrektur der Provisionierung von SAP Anreden	Ändert Property-Mapping-Regeln im Mapping title und user , um SAP Anreden in der korrekten Sprache zu provisionieren.	33423

Patch ID	Patch	Beschreibung	Fehler ID
		Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	

Tabelle 19: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33259_	Anzeigename des SCIM Referenzscopes	Korrigiert den Anzeigenamen des Referenzscopes.	33259

Patches in One Identity Manager Version 8.1.3

Tabelle 20: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32781_	Korrektur der Variable DefaultUserPassword	Korrigiert Sicherheitseinstellungen der Variable DefaultUserPassword. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32781

Tabelle 21: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32965	Korrektur des Scopefilters für ADSSite	Korrigiert den Scopefilter für ADSSite. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32965

Tabelle 22: Patches für Active Roles

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32844	Unterstützung für Funktionsebene Windows Server 2016	Fügt die Funktionsebene für Windows Server 2016 Domänen ein.	32844
VPR#32871	Negierung von TSInheritInitial Program entfernen	Korrigiert das Mapping der Schemaeigenschaft edsaWTSUserConfig InheritInitialProgram im Mapping User, da der Wert nicht mehr negiert werden muss.	32871

Tabelle 23: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32781_ EBS	Korrektur der Variable DefaultUserPassword	Korrigiert Sicherheitseinstellungen der Variable DefaultUserPassword. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32781

Tabelle 24: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32703	One Identity Manager Service Benutzerkonto für die Verbindung zulassen	Erlaubt die Verbindung mit dem Benutzerkonto des One Identity Manager Service.	32703

Tabelle 25: Patches für IBM Notes

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32781_ NDO	Korrektur der Variable DefaultUserPassword	Korrigiert Sicherheitseinstellungen der Variable DefaultUserPassword. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32781

Tabelle 26: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32768	Korrektur des Mappings Mailbox Statistics (User/Shared)	Entfernt die Object-Matching-Regel Identifer <-> Identity aus dem Mapping Mailbox Statistics (User/Shared) .	32768

Tabelle 27: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32781_ SAP	Korrektur der Variable TempUserPassword	Korrigiert Sicherheitseinstellungen der Variable TempUserPassword. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32781
VPR#33071	Änderung des Referenzscopes für den Schematyp SAPLicence	Korrigiert den Referenzscope für den Schematyp SAPLicence in der One Identity Manager-Verbindung.	33071

Patch ID	Patch	Beschreibung	Fehler ID
	(Teil 2)	Abhängig von Patch VPR#31930 (Änderung des Referenzscope für den Schematyp SAPLicence). Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	

Tabelle 28: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32899	Korrektur des Filters an der Schemaklasse HRPerson_0709_IDEXT	Ändert die Objektbestimmung der Schemaklasse HRPerson_0709_IDEXT. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32899

Tabelle 29: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32754	Korrektur der Property-Mapping-Regel vrtPrimary <-> primary	Ergänzt eine Bedingung an der Property-Mapping-Regel vrtPrimary <-> primary im Mapping User.	32754

Patches in One Identity Manager Version 8.1.2

Tabelle 30: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32258	Korrigiert das Mapping der Schemaeigenschaft vrtparentDn	Korrigiert die Property-Mapping-Regeln für das Mapping der Schemaeigenschaft vrtparentDn in allen Mappings, damit die Eigenschaften von Objekten, denen kein Container zugeordnet ist, korrekt provisioniert werden.	32258

Tabelle 31: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31928	Korrektur von Property-Mapping-Regeln im Mapping Calendar Processing (User/Shared)	Entfernt die Mappingregeln für AddNewRequestsTentatively und ProcessExternalMeetingMessages, da sie Fehler verursachen, wenn sie an das Cmdlet Set-Calendarprocessing übermittelt werden.	31928

Tabelle 32: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32667	Löschen der alternativen Object-Matching-Regel aus dem Mapping oRA-Requestgroup	Löscht die Object-Matching-Regel Identifizier <-> REQUEST_GROUP_ID aus dem Mapping oRA-Requestgroup . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32667
VPR#30464_1	Korrektur der Unterstützung von Oracle Database Editionen	Entfernt die Variable CP_EBSEdition aus dem Standardvariablen-set. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	30464

Tabelle 33: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32031	Anwenden einer virtuellen Appliance ID in allen Mappings	Setzt eine virtuelle Appliance ID im Konnektorschema und wendet diese in allen Mappings an. Abhängig von Patch Ersetzt Appliance serial als Applian-cekennung durch eine kunden-definierte Kennung (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32031
VPR#32423	Erweiterungen für die Synchronisation von PAM Authentifizierungsanbietern	Legt ein Mapping und einen Synchronisationsworkflow für AuthenticationProvider an und korrigiert die Mappings User und UserGroup . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. WICHTIG: Beim Anwenden des	32423

Patch ID	Patch	Beschreibung	Fehler ID
		<p>Patches gehen Daten verloren.</p> <p>Um diese Daten wiederherzustellen, starten Sie eine vollständige Synchronisation, unmittelbar nachdem die automatischen Patches angewendet wurden.</p>	

Tabelle 34: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32415	Neu Variable für SNC Login mit Benutzername und Kennwort	<p>Legt die Variable CP_sncsso im Standardvariablenst an.</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	32415
VPR#32584	Behandlung von SAP Anreden mit Sprachcode	<p>Aktualisiert das Konnektorschema, um die vollständige Liste der SAPTitle für jede Sprache einzulesen.</p> <p>Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.</p>	32584

Tabelle 35: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32154	Aktivierung der Revisionsfilterung	<p>Aktiviert die Revisionsfilterung in den Synchronisationsschritten Master Identity, Workdates of Employee und Communication Data.</p>	32154

Patches in One Identity Manager Version 8.1.1

Tabelle 36: Patches für Azure Active Directory

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

Tabelle 37: 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 38: 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 Raumpostfächern	Der Patch sorgt dafür, dass auch bei LinkedRoomMailboxes die Schemaeigenschaften LinkedCredential, LinkedDomainController und LinkedMasterAccount an den Konnektor übergeben werden.	30964

Tabelle 39: 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 40: 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 41: Patches für IBM Notes

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31420	Setzt Regelfilter an verschiedenen Synchronisationsschritten im Provisionierungsworkflow	Legt auszuschließende Regeln an den Synchronisationsschritten Certifier und Policy im Provisionierungsworkflow fest. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31420

Tabelle 42: 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 Applian- cekenennung durch eine	Ersetzt Appliance serial als eindeu- tige Kennung des Basisobjekts durch eine kundendefinierte Kennung und	31568

Patch ID	Patch	Beschreibung	Fehler ID
	kundendefinierte Kennung (Teil 1)	wendet diese Änderung in der Konfiguration des Synchronisation an. Voraussetzung für Patch Ersetzt Appliance serial als Appliancenummer durch eine kundendefinierte Kennung (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
VPR#31568B	Ersetzt Appliance serial als Appliancenummer 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 des Synchronisation an. Abhängig von Patch Ersetzt Appliance serial als Appliancenummer durch eine kundendefinierte Kennung (Teil 1) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31568
VPR#31569	Verbesserungen für One Identity Safeguard Cluster	Fügt Verbindungsparameter und Variablen für die Verbindung von One Identity Safeguard Clustern hinzu. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. 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.	31569
VPR#31664A	Änderungen für Zugriffsanforderungsrichtlinien für den Sitzungszugriff (Teil 1)	Eine Zugriffsanforderungsrichtlinie kann mehrere Verzeichniskonten für Sitzungszugriffe erhalten. Voraussetzung für Patch Änderungen für Zugriffsanforderungsrichtlinien für den Sitzungszugriff (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager	31664

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

Tabelle 43: 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 Referenzscope für den Schematyp SAPLicence	Korrigiert den Referenzscope für den Schematyp SAPLicence in der One Identity Manager Verbindung.	31930

Tabelle 44: 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 45: 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

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31756	Scope für Zugriffstoken	Erstellt einen Scope für Zugriffstoken als neuen Verbindungsparameter.	31756

Patches in One Identity Manager Version 8.1

Tabelle 46: Allgemeine Patches

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

Tabelle 47: Patches für Azure Active Directory

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

Tabelle 48: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#29087	Hinzufügen der Schemaeigenschaft mS-DS-ConsistencyGuid	Fügt die Schemaeigenschaft mS-DS-ConsistencyGuid in die Mappings User und InetOrgPerson ein.	29087
VPR#29306	Korrektur der Schema-klasse ADSSite (all) (Teil 1)	Ändert den Fremdschlüssel für ADSSite von ADSDomain zu ADSForest. Voraussetzung für Patch Korrektur der Schemaklasse ADSSite (all) (Teil 2) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	29306
VPR#29306_2	Korrektur der Schema-klasse ADSSite (all) (Teil 2)	Ändert den Fremdschlüssel für ADSSite von ADSDomain zu ADSForest. Abhängig von Patch Korrektur der Schemaklasse ADSSite (all) (Teil 1) . Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	29306
VPR#30192	Definition eines Scopes	Fügt einen Scope hinzu und die	30192

Patch ID	Patch	Beschreibung	Fehler ID
	und Nutzung der Verarbeitungsmethode MarkAsOutstanding	Verarbeitungsmethode MarkAsOutstanding in den Synchronisationsschritt trustedDomain ein.	
	Meilenstein 8.1	Meilenstein für den Kontext Active Directory .	

Tabelle 49: Patches für Active Roles

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

Tabelle 50: 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 Synchro-	Ergänzt einen Synchro-	29741

Patch ID	Patch	Beschreibung	Fehler ID
	nisationskonfiguration um HR PersonPrimaryLocation	nisationsschritt und ein Mapping für die Synchronisation des primären Standorts von Personen.	
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	Meilenstein für den Kontext Oracle E-Business Suite .	

Tabelle 51: Patches für Microsoft Exchange

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

Tabelle 52: 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	30498

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

Tabelle 53: Patches für G Suite

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

Tabelle 54: Patches für LDAP

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

Tabelle 55: Patches für IBM Notes

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

Tabelle 56: Patches für SAP R/3

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

Tabelle 57: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

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

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

Tabelle 58: Patches für SAP R/3 BI Analyseberechtigungen

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

Tabelle 59: Patches für SAP R/3 Berechtigungsobjekte

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

Tabelle 60: Patches für SharePoint

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

Tabelle 61: 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	Meilenstein für den Kontext SharePoint Online .	

Tabelle 62: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

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

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

Tabelle 63: Patches für die Universal Cloud Interface-Schnittstelle (im Modul Cloud Systems Management)

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

Tabelle 64: Patches für Unix

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

Tabelle 65: Patches für den One Identity Manager Konnektor

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

Tabelle 66: Patches für den CSV-Konnektor

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

Abgekündigte Funktionen

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

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

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

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

- 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 HINWEIS: Aus Performancegründen wird der Einsatz von 16 physischen Kernen empfohlen.
Arbeitsspeicher	16 GB+ RAM
Freier Festplattenspeicher	100 GB
Betriebssystem	Windows Betriebssysteme <ul style="list-style-type: none"> • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. UNIX und Linux Betriebssysteme <ul style="list-style-type: none"> • Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.
Software	Unterstützt werden die Versionen: <ul style="list-style-type: none"> • SQL Server 2016 Standard Edition (64-Bit), Service Pack 2

mit aktuellem kumulativen Update

- SQL Server 2017 Standard Edition (64-Bit) mit aktuellem kumulativen Update
- SQL Server 2019 Standard Edition (64-Bit) mit aktuellem kumulativen Update

HINWEIS: Das kumulative Update 2 für SQL Server 2019 wird nicht unterstützt.

- Kompatibilitätsgrad für Datenbanken: SQL Server 2016 (130)
- Standard-Sortierschema: Case-Insensitiv, SQL_Latin1_General_CP1_CI_AS (Empfehlung)

HINWEIS: Aus Performancegründen wird dringend der Einsatz der SQL Server Enterprise Edition empfohlen.

Minimalanforderungen für Dienstserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	16 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: <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 Linux Betriebssysteme <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	Windows Betriebssysteme <ul style="list-style-type: none">• Microsoft .NET Framework Version 4.7.2 oder höher <p>HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers.</p>

Linux Betriebssysteme

- 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	Windows Betriebssysteme <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	Windows Betriebssysteme <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

Linux Betriebssysteme

- Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden. Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für Apache HTTP Server.

Zusätzliche Software

Windows Betriebssysteme

- Microsoft .NET Framework Version 4.7.2 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:
 - 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)

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 67: Unterstützte Datensysteme

Konnektor	Unterstützte Datensysteme
Konnektor für Trennzeichen getrennte Textdateien	Beliebige durch Trennzeichen getrennte Textdateien.
Konnektor für relationale Datenbanken	Beliebige relationale Datenbanken, die ADO.NET unterstützen. HINWEIS: Die zusätzliche Installation eines ADO.NET Datenproviders eines Drittanbieters kann erforderlich sein. Wenden Sie sich an Microsoft oder den Hersteller der relationalen Datenbank.
Generischer LDAP Konnektor	Beliebiger LDAP Version 3 konformer Verzeichnisserver. Der LDAP Konnektor erfordert, dass sich die Verzeichnisserver RFC-konform verhalten. Insbesondere sind die Anforderung von RFC 4514 (String Representation of Distinguished Names) und RFC 4512 (Directory Information Models) zu gewährleisten. HINWEIS: Abhängig vom Schema können weitere Anpassungen bezüglich des Schemas und der Provisionierungsprozesse erforderlich sein.
Web Service Konnektor	Beliebige SOAP Web Services, die eine wsdl zur Verfügung stellen. HINWEIS: Es kann der Web Service Assistent benutzt werden,

Konnektor	Unterstützte Datenysteme
	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.
Active Directory Konnektor	Active Directory, welches mit Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019 ausgeliefert wird.
Microsoft Exchange Konnektor	<ul style="list-style-type: none"> • Microsoft Exchange 2010 ab Service Pack 3 • Microsoft Exchange 2013 mit kumulativem Update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 mit kumulativem Update 1 • MicrosoftExchange 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, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52 und 7.69 • SAP ECC 5.0 und 6.0 • SAP S/4HANA On-Premise-Edition
Unix Konnektor	Unterstützt werden die gängigsten Unix und Linux Derivate. Weitere Informationen finden Sie in den Spezifikationen für Authentication Services .
IBM Notes Konnektor	<ul style="list-style-type: none"> • IBM Domino Server Version 8, 9 und 10 • HCL Domino Server Version 11 • IBM Notes Client 8.5.3 und 10.0 • HCL Notes Client Version 11.0.1
Nativer Datenbankkonnektor	<ul style="list-style-type: none"> • SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW)

Konnektor	Unterstützte Datensysteme
	<ul style="list-style-type: none"> • 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, 7.3.3, 7.4.1 und 7.4.3
Azure Active Directory Konnektor	<ul style="list-style-type: none"> • Microsoft Azure Active Directory <p>HINWEIS: Die Synchronisation von Microsoft Azure China mit dem Azure Active Directory Konnektor wird nicht unterstützt. Weitere Informationen finden Sie unter https://support.oneidentity.com/KB/312379.</p>
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, 2.8, 2.9, 2.10, 2.11 und 6.0

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 8.1.4 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 57.

Hinweise zur Aktualisierung des One Identity Manager

- Stellen Sie vor der Aktualisierung der One Identity Manager-Datenbank auf die Version 8.1.4 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 8.1.4 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 8.1.4 funktioniert nur, wenn mindestens das Service Pack 7.1.3 installiert ist.
- One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe. Der Datenbankserver muss die extreme Transaktionsverarbeitung (XTP) unterstützen. Ist XTP nicht aktiviert, wird die Installation oder Aktualisierung nicht gestartet. Prüfen Sie, ob für den SQL Server die Eigenschaft **Extreme Transaktionsverarbeitung unterstützt** (Is XTPSupported) auf den Wert **True** gesetzt ist.

Für die Erstellung speicheroptimierter Tabellen sind folgende Voraussetzungen zu erfüllen:

- Es muss eine Datenbankdatei mit den Dateityp **Filestream-Daten** (Filestream data) vorhanden sein.
- Es muss eine speicheroptimierte Datendateigruppe (Memory-optimized data filegroup) vorhanden sein.

Vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank prüft der Configuration Wizard, ob diese Anforderungen erfüllt sind. Es werden im Configuration Wizard Reparaturmethoden angeboten, um die Datenbankdatei und die Datendateigruppe zu erstellen.

- Während der Aktualisierung einer One Identity Manager-Datenbank der Versionen 7.0, 7.1 oder 8.0 auf die Version 8.1.4 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 8.1.4 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 8.1.4 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 8.1.4

WICHTIG: Beachten Sie die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 57.

Um eine bestehende One Identity Manager Installation auf die Version 8.1.4 zu aktualisieren

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

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

HINWEIS: Um eine One Identity Manager History Database-Installation zu

aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.

- c. Klicken Sie **Installieren**.

Der Installationsassistent wird gestartet.

- d. Folgen Sie den Installationsanweisungen.

WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.

3. (von Version 7.0.x oder Version 7.1.x) Beenden Sie den One Identity Manager Service auf dem Server, der die direkten Anfragen der Datenbank verarbeitet.
(von Version 8.0.x 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 8.1.4 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 8.1.4 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.

HINWEIS: Nach der Aktualisierung einer One Identity Manager History Database-Installation von Version 7.0.x oder Version 7.1.x ist der One Identity Manager History Service nicht registriert.

Registrieren Sie den Dienst manuell. Führen Sie in der Kommandozeile im administrativen Kontext folgende Aufrufe aus:

```
sc create "HDBService" binpath= "<path>\vinetworkservice.exe"  
displayname= "One Identity Manager History Service"  
  
sc description "HDBService" "One Identity Manager History Service"
```

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 8.1.4 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 63.

Um einen Anwendungsserver auf die Version 8.1.4 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 8.1.4 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 8.1.4 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 8.1.4 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 8.1.4 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.**

HINWEIS: Beim Aktualisieren bestehender Synchronisationsprojekte werden immer die Verbindungsparameter aus dem Standardvariablenst set verwendet. Stellen Sie sicher, dass die Variablen im Standardvariablenst set gültige Werte enthalten.

HINWEIS: Wenn Sie Synchronisationsprojekte für die Anbindung von Cloud-Anwendungen im Universal Cloud Interface eingerichtet haben, aktualisieren Sie in diesen Synchronisationsprojekten das Zielsystemschem a, 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 28
- [Patches für Synchronisationsprojekte](#) auf Seite 29

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 2019.0001.0021.0400 für alle Module und die Anwendungsversion 8.1 2019-01-21-396 weisen darauf hin, dass diese Version installiert ist.

Zusätzliche Ressourcen

Zusätzliche Informationen sind verfügbar unter:

- [One Identity Manager Support](#)
- [One Identity Manager Online-Dokumentation](#)
- [One Identity Manager 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, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie <https://www.oneidentity.com/company/contact-us.aspx>.

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 2020 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 ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.