One Identity Manager 9.0

Versionshinweise

08. August 2022, 15:59 Uhr

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 9.0 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 8.2.1 aufgeführt.

One Identity Manager 9.0 ist ein LTS Release mit neuen Funktionen und verbessertem Verhalten. Siehe Neue Funktionen auf Seite 2 und Verbesserungen auf Seite 10.

VORSICHT: Bevor Sie eine bestehende One Identity Manager Installation auf die Version 9.0 aktualisieren, beachten Sie folgende Hinweise:

- **One Identity Manager 9.0 ist eine Weiterentwicklung der Version 8.2.1. Alle offiziellen Releases der Versionen 8.2.1, 8.1.5 oder älter sind geeignet für die Aktualisierung auf Version 9.0. Die Aktualisierung neuerer Versionen kann zu einem Downgrade führen.**
- **Für One Identity Manager 9.0 werden nur ausgewählte, von One Identity definierte Patches zur Verfügung gestellt. Ein Hotfix außerhalb dieser Definition, welcher für eine andere Version zur Verfügung gestellt wurde, wird somit nicht für das Release 9.0 zur Verfügung stehen.**

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.2.1 ist, lesen Sie auch die Versionshinweise der vorangegangenen Versionen. Die Versionshinweise sowie Versionshinweise zu zusätzlichen Modulen, die auf der One Identity Manager-Technologie basieren, finden Sie unter One Identity Manager Support.

Die One Identity Manager Dokumentation liegt sowohl in englischer als auch deutscher Sprache vor. Für die nachfolgend einzeln 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 9.0

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 ManagerActive Directory Edition umsetzen,
- Access Governance Anforderungen in Ihrem gesamten Konzern plattformübergreifend mit dem One Identity Manager verwirklichen.

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

One Identity Starling

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

Neue Funktionen

Neue Funktionen in One Identity Manager 9.0.

Allgemein

- Azure SQL-Datenbank wird unterstützt.

  HINWEIS: Für die Schemainstallation muss eine Azure SQL-Datenbank bereitgestellt werden. Das Erstellen einer neuen Azure SQL-Datenbank im Configuration Wizard wird nicht unterstützt.

- Die Verarbeitung der internen DBQueue Prozessor Aufträge erfolgt durch einen Dienst, den Database Agent Service. Der Database Agent Service wird über ein Plugin des One Identity Manager Service bereitgestellt. Das DatabaseAgentPlugin sollte auf dem Jobserver konfiguriert sein, der die Funktion des Aktualisierungsservers übernimmt. Für die Datenbankverbindung im Jobprovider muss ein administrativer Benutzer verwendet werden. Alternativ kann der Database Agent Service über das Kommandozeilenprogramm `DatabaseAgentServiceCmd.exe` ausgeführt werden.
- Der Configuration Wizard unterstützt Sie beim Löschen einer One Identity Manager-Datenbank. Beim Löschen einer Datenbank werden ebenfalls die Datenbankbenutzer, die Datenbankrollen und Serverrollen sowie die SQL Server Anmeldungen entfernt.
- Der Configuration Wizard unterstützt Sie beim Aktivieren einer wiederhergestellten Datenbank. Es werden die benötigten Datenbankbenutzer, Datenbankrollen und Serverrollen erzeugt sowie die Datenbank kompiliert.
- Aus Sicherheitsgründen können von den Frontends und Webanwendungen keine direkten Datenbankanfragen ausgeführt werden. Definierte SQL-Operatoren werden mit einem Risiko bewertet, so dass diese nicht über die One Identity Manager-Komponenten verwendet werden können. Dazu gehören beispielsweise `LIKE`, `NOT LIKE`, `<`, `<=`, `>` oder `>=`.

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

  Benutzer, die diese Programmfunktion nicht besitzen, können nur Datenbankabfragen ausführen, die als vertrauenswürdig eingestuft sind oder kein Risiko darstellen. Einige der Funktionen in den One Identity Manager-Komponenten, wie beispielsweise das Testen von dynamischen Rollen oder die Ausführung von Filterabfragen, sind ohne die Programmfunktion nicht möglich. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
- Mit dem Plugin **SessionHttpAuthentication** für den One Identity Manager Service wird die Anmeldung mit den Authentifizierungsmodulen an der Webseite des Dienstes unterstützt. Die Benutzer benötigen weiterhin die Programmfunktion **JobServer_Status**.
- Die Deaktivierung von WHERE-Klauseln für die REST-API des Anwendungsservers wird unterstützt.
- Diverse Kennwortspalten wurden verlängert.

- Für Kennwortrichtlinien kann für Kennwortanforderungen, die im Testskript geprüft werden, zusätzlich eine Beschreibung erfasst werden. Diese wird in der Beschreibung einer Kennwortrichtlinie im Kennwortrücksetzungsportal angezeigt.
- Systembenutzer können für die direkte Anmeldung an den One Identity Manager-Werkzeugen gesperrt werden.
- Es wird ein neues Authentifizierungsmodul **Benutzerkonto (manuelle Eingabe/rollenbasiert)** bereitgestellt. Zur Anmeldung wird die Person verwendet, deren eingetragene Anmeldung mit den Anmeldeinformationen des angemeldeten Benutzers übereinstimmt.
- Die Authentifizierungsmodule für das Kennwortrücksetzungsportal können eine Liste von Spalten derselben Tabelle nutzen, um nach einem Benutzer zu suchen.
- Im Database Transporter können jetzt mehrere Transportpakete zu einem kumulativen Transportpaket zusammengefasst werden.
- Um im Job Queue Info Prozessschritte mit dem Status **Frozen** zu reaktivieren, benötigen die Benutzer die Programmfunktion **JobQueue_Frozen**.
- Die Optimierung des Suchindex kann manuell auf dem Anwendungsserver gestartet werden.
- Im Standardverbindungsdialog für die One Identity Manager-Werkzeuge kann ein Verbindungs-Timeout festgelegt werden.
- Neuer optionaler Parameter im Kommandozeilenprogramm `DBCompilerCMD.exe`, um nur geänderte Teile des Systems zu kompilieren.
- Neue Prozessfunktion `Execute SQL Single` für die Prozesskomponente `SQLComponent` zur Ausführung von SQL -Anweisungen in einer einzelnen Instanz. Die Prozessfunktion kann verwendet werden, wenn ein spezieller Prozeduraufruf oder eine spezielle Datenänderung explizit nur in einer Instanz laufen darf.
- An Parametern kann ein Skript für Wertänderungen hinterlegt werden (`DialogParameter.OnPropertyChangedScript`), welches dynamisch ermittelt, ob ein Parameter beispielsweise nur lesbar oder ein Pflichtparameter ist.
- Integration der Ereignisse in die Typed-Wrapper-Klassen.
- Unterstützung von NLog 5.0.
- Unterstützung von Microsoft .NET Framework Version 4.8.
- Die One Identity Manager History Database wurde wesentlich vereinfacht, um einerseits den Aufwand für das Einrichten und Betreiben der Datenbank zu verringern und andererseits den Betrieb auch auf Azure SQL-Datenbanken zu ermöglichen. Die History Database stellt nur noch eine einfache Datenablage dar. Die History Database beinhaltet weder die One Identity Manager Module noch Daten zur Systemkonfiguration. Es gibt keine aktiven Komponenten mehr.

  Für die Datenübernahme geben Sie die One Identity Manager History Database in der One Identity Manager-Datenbank im TimeTrace bekannt.

  | WICHTIG:

- Es wird empfohlen, eine neue History Database zu installieren!
- Bestehende Datenbanken werden weiterhin für die Abfrage archivierter Daten im TimeTrace und in Berichten unterstützt. Diese Datenbanken müssen nicht migriert werden.
- Sollten Sie dennoch eine bestehende History Database migrieren wollen, beachten Sie, dass bei der Migration einer bestehenden History Database alle Funktionen, Prozeduren, Tabellen und Views gelöscht werden, die nicht in folgender Liste sind:

  HistoryChain, HistoryJob, ProcessChain, ProcessGroup, ProcessInfo, ProcessStep, ProcessSubstitute, RawJobHistory, RawProcess, RawProcessChain, RawProcessGroup, RawProcessStep, RawProcessSubstitute, RawWatchOperation, RawWatchProperty, SourceColumn, SourceDatabase, SourceTable, WatchOperation, WatchProperty

  Sichern Sie vor der Migration eventuelle kundenspezifische Erweiterungen.

Web Portal (API Server)

- Für die Multifaktor-Authentifizierung bei der Entscheidung von Bestellungen oder bei Attestierungen wird OneLogin genutzt. Voraussetzungen dafür sind:
  - Die Synchronisation mit einer OneLogin Domäne ist eingerichtet und die Umgebung wurde initial synchronisiert.
  - Der Wert des Konfigurationsschlüssels **ServerConfig/ITShopConfig/StepUpAuthenticationProvider** ist **OneLogin MFA**.
  - In der Konfigurationsdatei des API Servers (`web.config`) muss folgender Eintrag in den Connection String eingefügt werden:

    ```
    <add name="OneLogin"
    connectionString="Domain=<domain>;ClientId=<clientid>;ClientSecret=<cli
    entSecret>" />
    ```

    Die entsprechenden Werte sind der Konfiguration von OneLogin zu entnehmen.
- Der Empfänger einer Bestellung muss den Nutzungsbedingungen zustimmen, falls er für die Bestellung auch als Entscheider ermittelt wird.
- Der Besteller wird aufgefordert, den Nutzungsbedingungen für eine Leistungsposition zuzustimmen.
- Ein Besteller kann im Web Portal optionale Leistungspositionen bestellen.
- Im Web Portal können an der Übersicht einer Rolle die historischen Änderungsdaten für die Rolle angezeigt werden.
- Im Web Portal können nun gelöschte Rollen wiederhergestellt werden.
- Im Web Portal können zwei Rollen zu einer Rolle zusammengefasst werden. Diese Funktion wird für Abteilungen, Standorte, Kostenstellen und Geschäftsrollen angeboten.

- Es ist im Web Portal möglich, Bestellvorlagen im IT Shop zu pflegen und zur Erstellung neuer Bestellungen zu verwenden.
- Ausnahmegenehmiger können im Web Portal Richtlinienverletzungen genehmigen und ablehnen.
- Im Administrationsportal können Filter für Spalten und Tabellen zur Objektauswahl definiert werden.
- Administratoren und Eigentümer von Anwendungen im Application Governance Modul können Systemberechtigungen, die eine bestimmte Bedingung erfüllen, automatisch an Anwendungen zuweisen lassen. Eigentümer und Administratoren können benachrichtigt werden, wenn ihren Anwendungen automatisch neue Systemberechtigungen zugewiesen wurden.
    - Im Konfigurationsparameter **QER | ITShop | MailTemplateIdents | InformAboutApplicationEntitlements** kann die Mailvorlage konfiguriert werden, die für E-Mail-Benachrichtigungen an die Administratoren und Eigentümer von Anwendungen genutzt werden soll.
- Im Web Portal können Attestierern und Entscheidern von Bestellungen Entscheidungsempfehlungen gegeben werden. Die Empfehlungen zur Genehmigung oder Ablehnung von Attestierungsvorgängen oder Bestellungen werden anhand verschiedener Kriterien berechnet. Die Kriterien werden an den Konfigurationsparametern unterhalb von **QER | Attestation | Recommendation** und **QER | ITShop | Recommendation** spezifiziert.

Zielsystemanbindung

- Mit dem Offline-Modus kann die Verarbeitung zielsystemspezifischer Prozesse durch den One Identity Manager Service pausiert werden, wenn ein Zielsystem zeitweilig nicht erreicht werden kann. Damit wird verhindert, dass zielsystemspezifische Prozesse in der Jobqueue eingefroren werden und später manuell reaktiviert werden müssen.
- Für alle Spalten im One Identity Manager Schema können Einschränkungen für die Synchronisation dieser Spalten definiert werden. Dafür wird im Designer die Spalteneigenschaft **Synchronisationsinformationen** angezeigt.
- Synchronisations- und Provisionierungsprozesse werden zurückgestellt, solange die Synchronisationsprojekte aktualisiert werden.

  Die Wartezeit für Wiederholversuche wird im Konfigurationsparameter **Common | Jobservice | RedoDelayMinutes** eingestellt.
- Die Remoteunterstützung für Zielsystemverbindungen wird mit .net Core Mitteln umgesetzt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34646_SAP bereitgestellt.
- Unterstützung von OneLogin als Zielsystem.

  Der One Identity Manager konzentriert sich auf die Einrichtung und Bearbeitung von Benutzerkonten und die Versorgung mit den benötigten Berechtigungen für den Zugriff auf Anwendungen und für die Authentifizierung und Autorisierung. Im One

Identity Manager werden die OneLogin Benutzerkonten, Rollen und Anwendungen abgebildet. Die Synchronisation mit OneLogin übernimmt der OneLogin Konnektor. Der Zugriff auf die OneLogin Daten erfolgt über die OneLogin API. Mit der Installation des OneLogin Moduls wird eine Synchronisationsvorlage bereitgestellt. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung von OneLogin Domänen*.

- Die Zuweisung von Azure Active Directory Gruppen an Administratorrollen wird im One Identity Manager abgebildet.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33400 bereitgestellt.

- Regeln für Mitgliedschaften in dynamischen Azure Active Directory Gruppen werden in den One Identity Manager eingelesen.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34744 bereitgestellt.

- Die E-Mail-Adresse von Azure Active Directory Benutzerkonten kann jetzt im One Identity Manager bearbeitet und in das Zielsystem geschrieben werden.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35286 bereitgestellt.

- Der Erstellungstyp von Azure Active Directory Benutzerkonten wird in den One Identity Manager eingelesen.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35290 bereitgestellt.

- Azure Active Directory Verwaltungseinheiten werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35289 bereitgestellt.

- B2C Mandanten werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35033 bereitgestellt.

- Die Klassifizierung von Exchange Online Office 365 Gruppen wird unterstützt.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#35303_AAD und VPR#35303_O3E bereitgestellt.

- **TECH PREVIEW ONLY**: Der Exchange Online Konnektor unterstützt zertifikatsbasierte Authentifizierung.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34766 bereitgestellt.

  > WICHTIG: Diese Funktion kann in Testumgebungen getestet werden. Nutzen Sie die Funktion auf keinen Fall in einer produktiven Umgebung.

- Die Verschiebung von Active Directory Objekten über Domänengrenzen hinweg wird unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33793 bereitgestellt.

- Microsoft Exchange E-Mail aktivierte Verteilergruppen vom Typ **Raumliste** werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31374 bereitgestellt.
- Unterstützung von Active Roles 7.5.2, Active Roles 7.5.3 und Active Roles 7.6.
- Der Google Workspace Konnektor unterstützt die Synchronisation externer E-Mail-Adressen. Sie können als Mitglieder, Eigentümer oder Manager an Google Workspace Gruppen zugewiesen werden, für die externe Mitglieder zugelassen sind.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34885 bereitgestellt.
- Oracle E-Business Suite Version 12.2.10 wird unterstützt.
- One Identity Safeguard Version 7.0 wird unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35621 bereitgestellt.
- Es wird ein neuer Bericht mit einer Übersicht über die privilegierten Zugriffe der Mitarbeiter bereitgestellt.
- SharePoint Server Subscription Edition wird unterstützt.
- SAP Parameter können auch über Systemrollen an SAP Benutzerkonten vererbt werden.

Identity Management und Access Governance

- Verbesserte Unterstützung für die Vererbung von zielsystemspezifischen Gruppen. Es kann jetzt für einzelne Gruppen festgelegt werden, ob die Vererbungseinstellungen des Automatisierungsgrades für die Gruppe gelten oder ob die Einstellungen des Automatisierungsgrades für die Gruppe überschrieben werden. Damit kann beispielsweise definiert werden, dass eine Gruppe niemals automatisch von Benutzerkonten entfernt werden soll.
- Es werden neue Entscheidungsrichtlinien für die Bestellung und Attestierung von Azure Active Directory und Exchange Online Systemberechtigungen bereitgestellt.
- Der Objektschlüssel des effektiv zugewiesenen Produkts wird am Bestellvorgang gespeichert, wenn im Verlauf des Genehmigungsverfahrens das bestellte Produkt geändert wird.
- An Leistungspositionen, Servicekategorien und Entscheidungsschritten kann festgelegt werden, ob bei der Bestellung oder Entscheidung eine Begründung verpflichtend angegeben werden muss oder optional angegeben werden kann.
- Bestellungen können mit dynamischen Parametern versehen werden, deren Werte der Besteller erst direkt bei der Bestellung festlegt. Aus diesen Parametern und deren Werten wird nach der Genehmigung, eine Systemberechtigung (`UNSGroupB`) erzeugt und dem Bestellempfänger zugewiesen.
- Es werden weitere Standardobjekte für die Attestierung von Personen bereitgestellt. Diese Attestierungen können über einen Richtlinienverbund gemeinsam gestartet

werden.

- Identität selbst
- Primäre oder sekundäre Abteilungen
- Mitgliedschaften in Geschäfts- oder Systemrollen
- Verbundene Benutzerkonten
- Zugewiesene Systemberechtigungen

An Entscheidungsrichtlinien kann konfiguriert werden, ob diese beim Erstellen von Attestierungsrichtlinien im Web Portal ausgewählt werden können.

Zusätzliche Entscheidungsverfahren:

- CN - Anfechtung der Entscheidung
- PW - Eigentümer der Attestierungsrichtlinie
- XM - Manager der Person für alle Attestierungen

- Attestierungsrichtlinien, die zusammen ausgeführt werden sollen, können zu Richtlinienverbunden zusammengefasst werden. Über eine Stichprobe kann die Menge der zu attestierenden Objekte für alle Attestierungsrichtlinien im Verbund eingeschränkt werden.
- Wenn am Attestierungsverfahren kein Bericht angegeben ist, werden Snapshots erzeugt, welche die notwendigen Informationen über die zu attestierenden Objekte enthalten. Der Inhalt dieser Snapshots kann konfiguriert werden.

  HINWEIS: Der Snapshot wird durch das Skript `ATT_GetAttestationObject` erzeugt. Damit wird das Skript `VI_GetAttestationObject` ersetzt.
- An Anwendungen (Application Governance Modul) kann das Datum der nächsten Attestierung festgelegt werden. Es werden verschiedenen Standard-Attestierungsrichtlinien bereitgestellt, die dieses Datum nutzen.

Siehe auch:

- Verbesserungen auf Seite 10
- Gelöste Probleme auf Seite 15
- Schemaänderungen auf Seite 30
- Patches für Synchronisationsprojekte auf Seite 37

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die im One Identity Manager 9.0 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Für DBQueue Prozessor Aufträge kann eine minimalen Zeit bis zur Reaktivierung konfiguriert werden.	32015
Der Anwendungsserver unterstützt Session-Zertifikate, die mit der CNG-API erstellt wurden.	32138
Verbesserte Performance bei der Verarbeitung von DBQueue Prozessor Aufträgen.	34049
Verbesserte Fehlermeldung, wenn beim Signieren von E-Mails ein Fehler auftritt und verbesserte Dokumentation.	35226
Geänderte Werte können in der tabellarischer Anzeige mit einem Symbol gekennzeichnet werden. Die Konfiguration erfolgt über die den Dialog für die Darstellungseigenschaften.	35247
Verbesserte Anzeige der Statusseite des One Identity Manager Service.	35285, 33313
Verbesserte Anzeige der Statusseite des Anwendungsservers.	33314
Performance-Optimierung bei der Auswertung von Bedingungen.	35407
Über das Attribut `UnitOfWork` kann in den Skripten jetzt auf die aktuell geöffnete Unit of Work zugegriffen werden.	35417
Das Markieren von Where-Klauseln als vertrauenwürdig wurde verbessert.	35418
Die Eigenschaften **Proxyview** und **Erweiterungen zur Proxyview** werden im Schemaeditor jetzt auf dem Tabreiter **Weitere** angezeigt.	35613
Die Authentifizierung über LDAP über eine SSL-Verbindung zum LDAP Server wird unterstützt. Die Konfiguration erfolgt über die Konfigurationsparameter unterhalb von **TargetSystem | LDAP | AuthenticationV2**.	34453
Verbesserte Performance für die Generierung von Prozessen.	35134, 35152
Im Designer können jetzt in der Kategorie **Erste Schritte** administrative Systembenutzer erstellt werden.	35263
Verbesserte Zuweisung von Dateien an Maschinenrollen.	33271
Verbessertes Verhalten der Kommandozeilenwerkzeuge. Es werden	35427,

Verbesserung	Fehler ID
Basistests zur Parameterübergabe ausgeführt. Version, Fehlermeldungen und Hilfetexte werden ausgegeben.	34825
Verbesserte Performance bei der Ermittlung von Anzeigeberechtigungen.	35612
Verbesserte Performance bei der Anzeige der Prozesse im Job Queue Info.	35641
Zusätzlich zur Prozedur `QBM_ZDBQueueVoidTask` wird neu die Prozedur `QBM_ZDBQueueVoidTaskBulk` geliefert. Damit können jetzt auch DBQueue Prozessor Aufträge deaktiviert werden, die für die Bulkverarbeitung gekennzeichnet sind, indem man diese Prozedur in die Spalte `QBMDBQueueTask.ProcedureName` einträgt.	34864
Es wird ermöglicht, an der DB-Session in der VI.DB ein eigenes Query-Timeout zu setzen, was dann für alle Queries verwendet wird.	34917
Die Drittanbieterkomponente Microsoft.Graph wurde aktualisiert.	35025

Tabelle 2: Allgemein Webanwendungen

Verbesserung	Fehler ID
Im Web Portal werden dem Entscheider die Details zu den bestellten Leistungspositionen angezeigt. Falls eine Rollenmitgliedschaft bestellt wird, werden Informationen zu den Berechtigungen der Rolle angezeigt.	297243
Leistungspositionen werden zur Verbesserung der Performance im Web Portal nicht mehr sortiert ausgegeben. Dies betrifft unter anderem den Servicekatalog und die Auswahl bestellbarer Produkte.	309523
Die Regelverletzungen für eine bestimmte Regel können jetzt aus einem E-Mail-Link angezeigt werden.	253881
Verbesserte Generierung von Berichten über den API Server.	291080
Es soll über die API-Konfiguration einstellbar sein, ob bei der Bestellung über einen Referenzbenutzer nur bestellte Berechtigungen und Zuweisungen angeboten werden oder alle Zuweisungen, die der Referenzbenutzer besitzt. In der Standardeinstellung werden nur bestellte Objekte angezeigt. Falls genau ein Bestellempfänger gewählt ist, ist dieser Bestellempfänger nicht als Referenzbenutzer auswählbar.	33551, 295703
Die Verwendung des ImxClient-Kommandozeilenprogramms unterstützt nun ein Software Update. Das ImxClient-Kommando `start-update` kann verwendet werden, um ein Software Update zu starten.	310595
Die Erkennung von sicheren Verbindungen unterstützt nun die Verwendung von HTTPS-to-HTTP Reverse Proxies.	313545
Die Konfiguration des Cookie-Pfads für das Anti-XSRF-Cookie kann angepasst werden.	35620, 310602
Für jede entity-basierte API-Methode kann eine einschränkende Filter-	311030

Verbesserung	Fehler ID
bedingung in der Konfiguration angegeben werden.	
Das TypeScript-Interface `IEntity` wurde um eine Methode `MarkForDeletion()` erweitert.	288697

Die folgenden ImxClient-Kommandos werden geändert:
`get-filestate`
`fetch-files`
`push-files`
Für diese Kommandos ist `/targets` jetzt ein Pflichtparameter.
	310837

Angular wurde auf Version 13 aktualisiert. Daraus kann sich für angepassten HTML5-Code die Notwendigkeit zu manuellen Korrekturen ergeben.	310627
Der API Server prüft die definierten API-Routen beim Start auf Eindeutigkeit. Für nicht-eindeutige Routen wird eine Warnmeldung ausgegeben. Bei kundenspezifisch definierten Routen kann es sein, dass nun Warnmeldungen ausgegeben werden.	279209
Verbesserte Performance beim Auflisten der bestellbaren Servicekategorien im Web Portal.	35577
Für die Anzeige von Beziehungen auf Formularen kann optional das lange Anzeigemuster (`DialogTable.DisplayPatternLong`) für die hierarchische Darstellung verwendet wird.	35482
Der Trusted Source Key, mit dem für ein Web-Frontend festgelegt werden kann, dass Where-Klauseln aus dem Frontend als vertrauenswürdig eingestuft sind, kann jetzt als Option `ConnectionBehaviour/TrustedSourceKey` in der Konfigurationsdatei angegeben werden.	35239

Tabelle 3: Zielsystemanbindung

Verbesserung	Fehler ID
Ungenutzte virtuelle Schemaeigenschaften wurden aus dem Mapping `site` in Active Directory Synchronisationsprojekten entfernt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35533 bereitgestellt.	35533
Ein Fehler im Patch VPR#35343_EX0 wurde korrigiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35506 bereitgestellt.	35506
Der LDAP Konnektor ignoriert die Groß- und Kleinschreibung beim Wertevergleich in den Schemaeigenschaften `ObjectClass` und	35702

Verbesserung	Fehler ID
`StructuralObjectClass`. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35702 bereitgestellt.	
In Synchronisationsprojekten für Exchange Online- und SharePoint Online-Umgebungen wird verhindert, dass mehr als ein Basisobjekt angelegt werden. Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#30841 bereitgestellt.	30841
Quota-Einstellungen von Exchange Online Postfächern werden synchronisiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34568 bereitgestellt.	34568
Die Postfachberechtigungen **Vollzugriff** und **Senden als** von Exchange Online Postfächern werden synchronisiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34265 bereitgestellt.	34265
Verbesserte Darstellung von App-Registrierungen und Unternehmensanwendungen für Azure Active Directory im Manager.	35212
Verbesserter Unterstützung der automatischen Personenzuordnung für Azure Active Directory Benutzerkonten für Gastbenutzer.	35584
Für die Synchronisation von SAP HCM Personalplanungsdaten werden weitere Revisionsfilter genutzt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32154 bereitgestellt.	32154
Performanceverbesserungen im SCIM Konnektor. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34952 bereitgestellt.	34952, 34953, 34954
Bei der Einrichtung der Systemverbindung zu einer Cloud-Anwendung kann der Request Timeout für Anfragen an den SCIM Provider konfiguriert werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35571 bereitgestellt.	35571
In Skriptvariablen können Code-Ausschnitte verwendet werden. Im Synchronization Editor werden Beispiele für häufig verwendet Skriptvariablen bereitgestellt.	35011
Verbesserungen der Synchronization Engine.	35196, 35480,

Verbesserung	Fehler ID
• Fehlerbehandlung • Erkennung von Objekten, die für die Synchronisation gesperrt sind • Automatische Erkennung von irregulär abgebrochenen Synchronisationen	35617
Verbesserte Darstellung der zusätzlichen Informationen über das angebundene Zielsystem im Synchronization Editor.	35242
In der Kopfzeile von Provisionierungsprotokollen wird das geänderte Objekt angezeigt.	35493
Verbesserte Darstellung der Systemberechtigungen-erbbar-Optionen auf dem Stammdatenformular für Benutzerkonten.	35524
Verbesserungen des One Identity Manager Business Application Programing Interface.	35556
Verbesserte Darstellung von ausstehenden Objekten aus Zuordnungstabellen im Zielsystemabgleich.	34930
Verbesserte Darstellung zugewiesener SAP Gruppen, Rollen, Profile auf dem Überblicksformular für SAP Benutzerkonten.	34780
Verbesserte Aufzeichnung von Löschoperationen für dynamische Rollen.	35544
Performanceverbesserung bei der Synchronisation, wenn ein lokaler Cache genutzt wird.	34955
In die Dokumentation zur Anbindung einer SAP R/3-Umgebung mit BI Analyseberechtigungen wurde folgender Hinweis aufgenommen: HINWEIS: BI Analyseberechtigungen, die in der SAP R/3-Umgebung indirekt über SAP Rollen oder SAP Profile an SAP Benutzerkonten zugewiesen sind, werden im One Identity Manager nicht abgebildet. Mit entsprechend formulierten SAP Funktionen für das Berechtigungsobjekt `S_RS_AUTH` kann im Identity Audit dennoch geprüft werden, ob diese Zuweisungen von BI Analyseberechtigungen zulässig sind.	35295
Verbesserte Darstellung erbbarer Gruppen und Systemberechtigungen auf den Überblicksformularen für Cloud Benutzerkonten und Benutzerkonten in kundendefinierten Zielsystemen.	35508
Der AS/400 LDAP Konnektor wurde umbenannt in IBM i LDAP Konnektor.	35275
Im Funktionsbaustein `/VIAENET/READTABLE` wird die Ausführung von `LIKE`-Abfragen verhindert. • Um die Änderung anzuwenden, spielen Sie den BAPI-Transport `SAPTRANSPORT_70.ZIP` in das SAP R/3-System ein.	35741

Tabelle 4: Identity Management und Access Governance

Verbesserung	Fehler ID
Auf dem Überblicksformular für Personen wird auch der Mandant der verbundenen SAP Benutzerkonten angezeigt.	34929
Verbesserte Darstellung der Stammdaten von Attestierungsverfahren im Manager.	35576
An Leistungspositionen kann eingestellt werden, ob sie im Servicekatalog ausgeblendet werden sollen, auch wenn sie grundsätzlich bestellbar bleiben.	35031
Abgeschlossene Stellvertretungen können aus der Datenbank gelöscht oder archiviert werden.	35096
Die Ablaufzeit für adaptive Karten wurde auf 24 Stunden erhöht. Der Wert des Konfigurationsparameters **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** ist nun standardmäßig **86400**.	35727
Abgeschlossene Stellvertretungen werden durch den DBQueue Prozessor gelöscht, sobald die Aufbewahrungszeit der Stellvertretungen überschritten ist.	35096

Siehe auch:

- Schemaänderungen auf Seite 30
- Patches für Synchronisationsprojekte auf Seite 37

Gelöste Probleme

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

Tabelle 5: Allgemein

Gelöstes Problem	Fehler ID
Beim Definieren von Prozeduren kommt es sporadisch an unterschiedlichen Stellen zum Abbruch. Fehlermeldung: `error 2021: The referenced entity 'xxx' was modified during DDL execution. Please retry the operation.`	33544
Fehler bei Ausführung der Prozedur `QBM_PJobUpdateState_Bulk`: `There is insufficient system memory.`	34590
Neu ausgestellte Zertifikate werden unter Umständen nicht akzeptiert.	34900
Unter Umständen werden während der Prozessverarbeitung einander ausschließende Prozesse ausgeliefert.	34973

Gelöstes Problem	Fehler ID
Zeitpläne werden im Designer nicht korrekt sortiert.	35522
Änderung der Konfiguration des One Identity Manager Service per Job Service Configuration werden nicht immer in die Datenbank übertragen.	35538
Anzeigefehler auf dem Tabreiter Berechtigungen in den Objekteigenschaften im Manager.	35558
Wiederherstellen der Anmeldung bei abgelaufenen Sitzungen im Anwendungsserver funktioniert nicht.	35594
Fehler beim Verbinden mehrerer Designer-Instanzen über einen Anwendungsserver.	35668
Im Manager werden Methodendefinitionen angezeigt, obwohl die Sichtbarkeitsberechtigung über ein Skript entfernt wurde.	35507
Die Authentifizierung am Tokenendpunkt über die Methode **client_secret_post** muss die Client ID mitbringen.	35691
Prozessschritte der Prozesskomponente `DelayComponent` mit der Prozessfunktion `Delay` schlagen mit SQL-Syntaxfehler fehl.	35744
Die Installation eines Anwendungsservers schlägt fehl, wenn die Authentifizierung über einen Systembenutzer nicht erlaubt ist.	34875

Tabelle 6: Allgemein Webanwendungen

Gelöstes Problem	Fehler ID
Wenn im Einkaufswagen des Web Portals viele Produkte liegen, für die Parameter angegeben werden müssen, kommt es zu Fehlern.	34417
Im Web Portal wird beim automatischen Abbestellen von Produkten durch eine abgelehnte Attestierung eine falsche Begründung hinterlegt.	34528
Bei der Installation der Manager Webanwendung wird unnötigerweise WebView2 installiert.	35662
In der Vorschau im Web Designer tritt beim Öffnen einer Servicekategorie beim Bestellvorgang ein Fehler auf.	35404
Die OAuth Anmeldung am API Server schlägt fehl, weil der Parameter `State` nicht entschlüsselt werden kann.	35611
Die Anzeigenamen von Bestellpositionen werden nicht lokalisiert.	34865
Wenn keine passende Zeitzone ermittelt werden kann, kommt es im Web Designer Web Portal zu einer Fehlermeldung: `Sequence contains no matching element`.	35191
Wird im Web Designer Web Portal in einem Datumsfeld **Enter** gedrückt, dann wird zur Startseite navigiert.	35559

Gelöstes Problem	Fehler ID
Kennwortfragen im Web Portal noch unter **Profil** angezeigt, obwohl der dazugehörende Parameter den Wert **false** hat.	35647
Im Web Portal wird für die Beschreibung eines Produktes nicht der gesamte Text als Tooltip angezeigt, sondern die technische Bezeichnung.	35659
In der Knotenbearbeitung im Web Designer werden bei einigen Eigenschaften die Daten nicht angezeigt, sondern nur Scrollbalken.	35586
Im Kennwortrücksetzungsportal werden, nach einem fehlerhaften Anmeldeversuch, die Authentifizierungsmodule zur Anmeldung doppelt angezeigt.	35546
Die Suche im Administration-Portal liefert unter Umständen keine Ergebnisse.	307328
Bei einer Neuanmeldung der Datenbanksitzung innerhalb derselben API Server-Sitzung wird der zuvor verwendete Benutzer nicht abgemeldet.	306163
Der Suchindex aktualisiert die Stichwörter zu Objekten nicht.	303391
Der Suchindex findet Zeichenfolgen, die einen Bindestrich oder einen Backslash enthalten, nicht in jedem Fall.	35634
Bei der Anzeige von Attestierungsvorgängen im Web Portal werden die Überschriften der Spalten `Grouping` und `Property` nicht korrekt dargestellt.	35171
Bei Klick auf das angepasste Firmenlogo im Web Portal wird die Startseite nicht geöffnet.	35658

Tabelle 7: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Das Skript `DPR_NeedExecuteWorkflow` und die genutzte View `DPR_VWorkflowHandlesProperty` beachten die Mappingrichtung der gemappten Schemaeigenschaften nicht.	34982
Bei der Synchronisation einer Active Roles Domäne tritt ein Konvertierungsfehler auf. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35122 bereitgestellt.	35122
Bei der Synchronisation von Cloud-Anwendungen mit dem Universal Cloud Interface Konnektor werden die `UserInGroup*` und `UserHasGroup*` Tabellen nicht beachtet. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35451 bereitgestellt.	35451
Fehler beim Öffnen eines AdminP-Auftrags im Objektbrowser des Synchronization Editor, wenn keine Datenbankdatei angegeben ist.	35500

Gelöstes Problem	Fehler ID
Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35500 bereitgestellt.	
Beim Aktualisieren von Synchronisationsprojekten für eine Domino-Umgebung wird die Variable `MailFileAccessType` nicht korrekt angelegt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35745 bereitgestellt.	35745
Customizer verhindern das Speichern von Objekten, wenn die Spalte `XOrigin` den Wert **0** hat.	34854
Fehlerhafte Konvertierung von Werten in Custom Extensions.	35060
Der Anzeigename von Azure Active Directory Benutzerkonten für Gastbenutzer wird nicht in das Zielsystem übertragen.	35598
Der Merge-Modus für die Tabellen `AADApplicationOwner` und `AADServicePrincipalOwner` ist nicht aktiviert.	35183
Die Azure Active Directory Synchronisation bricht ab, wenn ein Eigentümer eines Dienstprinzipals selbst ein Dienstprinzipal ist. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35768 bereitgestellt.	35768
Microsoft Teams Teams und Microsoft Teams Kanäle sind keinem Scope zugeordnet. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35410 bereitgestellt.	35410
Der Erstellen von Microsoft Teams Kanälen scheitert.	35428
Gruppenmitgliedschaften von Active Directory Gruppen, die zum Löschen markiert sind, werden nicht entfernt.	35293
Rogue Correction von Active Directory Gruppenmitgliedschaften funktioniert nicht.	35492
Read-Prozesse für Active Directory nutzen den Parameter `OverrideVariables` nicht.	35555
Bei der automatischen Personenzuordnung wird unter Umständen ein unnötiges Remotepostfach erzeugt.	35146
Der Prozess `PAG_PAGAccessOrder_CheckExistingAccessRequest` schlägt fehl.	35593
Fehler beim Erstellen einen Unix Benutzerkontos, wenn der Nachname der verbundenen Person einen Doppelpunkt (**:**) enthält	26374
Das Nachladen von Objekten im Bulk-Modus scheitert, wenn ein Element nicht geladen werden kann.	34420

Gelöstes Problem	Fehler ID
Konvertierungsfehler bei der Synchronisation einer Active Directory Domäne über One Identity Active Roles.	35122
Wenn in einem Synchronisationsschritt mindestens drei Verarbeitungsmethoden definiert sind, wird die Reihenfolge der Verarbeitungsmethoden beim Speichern des Synchronisationsprojekts vertauscht.	35499
Die Dokumentation zur Einrichtung einer Systemverbindung mit einer Oracle Database ist nicht aktuell.	35505
Beim Einrichten der Systemverbindung mit einer SalesForce-Anwendung werden keine Schematypen erkannt.	35679
Fehler beim Verschlüsseln einer Datenbank, wen `DPRSystemConnection.ConnectionParameter` als verschlüsselt gekennzeichnet ist.	35695
Für Azure Active Directory Benutzerkonten funktioniert die Einzelobjektsynchronisation nicht mehr.	35728
Die Update-Migration einer sehr großen Datenbank wird nach 12 Stunden im Schritt `SAP 2019.0004.0017.0000 (31561)` abgebrochen.	35464
Wenn für Direktzuweisungen von SAP Rollen an SAP Benutzerkonten Bestellungen generiert werden, werden die Direktzuweisungen gelöscht und mit einem anderen Gültigkeitszeitraum neu erstellt.	35648
Fehler beim Anwenden des Patches VPR#34563.	35696
Auf dem Überblicksformular für Cloud-Anwendungen werden die zugeordneten Systemberechtigungen 1, 2 und 3 nicht angezeigt.	35512
Automatisch erstellte Benutzerkonten in kundendefinierten Zielsystemen oder Benutzerkonten (Tabelle `UNSAccountB`) oder Cloud Benutzerkonten (Tabelle `CMSUser`) erben keine Gruppen. Weitere Informationen finden Sie auch im Knowledge Artikel unter https://support.oneidentity.com/kb/339327.	35214

Tabelle 8: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Die Berechtigungen der Gruppe **vi_4_ITSHOPADMIN_OWNER** für Tabelle `AADGroup` sind fehlerhaft.	35519
Übersetzungen des Namens einer Anwendung werden nicht für die Servicekategorie übernommen.	35041
Die DBQueue Prozessor Aufträge `QER-K-ShoppingRackPWOHelperPWO-Del` und `ATT-K-AttestationHelper-Del` verursachen unter Umständen Blockaden.	35157

Gelöstes Problem	Fehler ID
Fehler beim Transportieren einer mehrfach bestellbaren Ressource.	35470
Fehlende Abhängigkeiten zwischen DBQueue Prozessor Aufträgen für die Zuweisung von Unternehmensressourcen zu Personen.	35294
Performanceprobleme bei der Ermittlung von Attestierungsobjekten (DBQueue Prozessor Auftrag `ATT-K-HelperAttestationPolicy`).	34201
Performanceprobleme bei der Neuberechnung der Attestierer.	35455
Wenn eine Entscheidungsebene mit mehreren Entscheidungsschritten aufgrund eines Timeouts abgelehnt wird, wird mitunter die nachfolgende Entscheidungsebene (bei Ablehnung) nicht ausgeführt.	35473, 35474
Obwohl ein Attestierungsvorgang im Hold-Status ist, erhalten Attestierer, die währenddessen für diesen Entscheidungsschritt neu ermittelt werden, eine Aufforderung zur Attestierung als E-Mail-Benachrichtigung. Im Manager und im Web Portal wird für diese Attestierer korrekterweise nichts zum Attestieren angezeigt.	35583
Die Complianceprüfung von Bestellungen im Warenkorb und im Genehmigungsverfahren erkennt keine Regelverletzung, wenn diese durch unterschiedliche Identitäten einer Person zustande kommt. Erst die zyklische Complianceprüfung erkennt die Regelverletzung.	35170
Performanceprobleme bei der Berechnung der von Complianceregeln betroffenen Personengruppen.	35261
Beim automatischen Entzug von Berechtigungen nach einer negativen Attestierung werden Bestellungen mit den Status **Verlängerung** und **Abbestellung** nicht berücksichtigt.	34725
Eine sofortige Abbestellung einer Bestellung ist nicht möglich, wenn diese Bestellung zuvor bereits mit einem Gültigkeitsdatum abbestellt wurde.	35431
Wenn der DBQueue Prozessor Auftrag `QER-K-ShoppingRackPWOHelperPWO` in mehreren Slots verarbeitet wird, wird dieser Auftrag unter Umständen immer wieder zurückgestellt. Andere Aufträge werden dadurch nicht verarbeitet.	35466
Beim Versenden von E-Mail-Benachrichtigungen in Genehmigungsverfahren von Bestellungen werden falsche Mailvorlagen verwendet.	35496
Die Mailvorlage **IT Shop Bestellung – Verlängerung** gibt unter **Bestellt durch** den Erstbesteller der Bestellung an, anstelle der Person, welche die Verlängerung bestellt.	35529
Bestellungen von Produkten, für die ein Gültigkeitszeitraum festgelegt ist, lassen sich unbegrenzt verlängern.	35651

Siehe auch:

- Schemaänderungen auf Seite 30
- Patches für Synchronisationsprojekte auf Seite 37

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
Header-Zeilen in als CSV gespeicherten Reporten enthalten keine sprechenden Namen.	24657
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, das keine unzulässigen Modulkombinationen ausgewählt werden.	25315
Fehler bei der Verbindung über einen Anwendungsserver, 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
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`	29535

Bekanntes Problem	Fehler ID
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.	
Wenn die One Identity Manager-Datenbank in einem SQL-Cluster (High Availibility Group) installiert ist und die Option `DTC_SUPPORT = PER_DB` gesetzt ist, erfolgt die Replikation zwischen den Servern mittels Distributed Transaction. Falls dabei ein `Save Transaction` ausgeführt wird, tritt ein Fehler auf: `Cannot use SAVE TRANSACTION within a distributed transaction.` Lösung: Deaktivieren Sie die Option `DTC_SUPPORT = PER_DB`.	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 *One Identity Manager Konfigurationshandbuch*.	31322
Bei der Installation der Datenbank unter SQL Server 2019 tritt ein Fehler auf: `QBM_PDBQueueProcess_Main unlimited is only allowed as an agent job` Lösung: • 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 `C:\inetpub\wwwroot`) 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,	32364

Bekanntes Problem	Fehler ID
kundenspezifischen Spalten gespeichert werden. 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 Bestel-leigenschaften für die verknüpfte Bestellung aus der identischen (kunden-spezifischen) 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. Workarounds: • 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**.	32938

Falls die Anwendung durch eigene DLL-Dateien ergänzt wird, kann es dazu kommen, dass eine falsche Version der Datei `Newtonsoft.Json.dll` geladen wird. Dadurch kann im Betrieb der Anwendung folgender Fehler auftreten:
`System.InvalidOperationException: Method may only be called on a Type for which Type.IsGenericParameter is true. at System.RuntimeType.get_DeclaringMethod()`
Für das Problem gibt es zwei mögliche Lösungen:
• Die eigenen DLLs werden gegen dieselbe Version der `Newtonsoft.Json.dll` kompiliert, um den Versionskonflikt zu beheben.
• In der entsprechenden Konfigurationsdatei (beispielsweise `web.config`) eine Assembly-Umleitung definieren.
Beispiel:
`<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1"> <dependentAssembly> <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30AD4FE6B2A6AEED" culture="neutral"/> <bindingRedirect oldVersion="0.0.0.0-11.0.0.0" newVersion="11.0.0.0"/> </dependentAssembly>`
	33867

Bekanntes Problem	Fehler ID
`</assemblyBinding>`	
Im Web Portal werden in der Detailanzeige eines offenen Attestierungsvorgangs nicht die erwarteten Felder angezeigt, wenn nicht das Standard-Attestierungsverfahren verwendet wird, sondern eine Kopie dessen. Lösung: • Die objektabhängigen Verweise des Standard-Attestierungsverfahrens müssen auch für das kundendefinierte Attestierungsverfahren übernommen werden.	34110

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 Domino Konnektor (`Error getting revision of schema type ((Server))`). Wahrscheinliche Ursache: Die HCL Domino-Umgebung wurde neu aufgebaut oder es wurden zahlreiche Einträge in das Domino-Verzeichnis eingefügt. Lösung: Aktualisieren Sie in der HCL Domino-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. 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.	27359
Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer	29253

Bekanntes Problem	Fehler ID
Zentralen Benutzerverwaltung. 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. 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.	29556
Der Zielsystemabgleich zeigt in der Manager Webanwendung keine Informationen an. Workaround: Nutzen Sie den Manager, um den Zielsystemabgleich durchzuführen.	30271
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: `400: Bad Request -- 60639: A valid account must be identified in the request.` Die Bestellung wird im One Identity Manager abgelehnt und der Fehler in der Bestellung als Begründung angezeigt.	796028, 30963
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. Ursache: Der SharePoint Konnektor lädt standardmäßig alle Objekteigenschaften in einen Cache. Lösung: • Korrigieren Sie den Fehler im Zielsystem.	31017

Bekanntes Problem	Fehler ID
- ODER - • Deaktivieren Sie den Cache in der Datei `VI.Projector.SharePoint.<Version>.Host.exe.config`.	
Wenn eine SharePoint Websitesammlungen nur lesbar ist, kann das Serverfarmkonto die Schemaeigenschaften `Owner`, `SecondaryContact` und `UserCodeEnabled` nicht lesen. 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.	31904

Wenn Datumsfelder in einer SAP R/3-Umgebung Werte enthalten, die kein 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>`
	32149

Die in der Prozesskomponente `PowershellComponentNet4` im Parameter `OutputFile` zu erzeugende Datei enthält keine Fehlermeldungen. Ursache:	32945

Bekanntes Problem	Fehler ID
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 Protokolldatei des One Identity Manager Service.	
Der Google Workspace Konnektor kann die Nutzerdaten von Google Applikationen vor dem Löschen eines Benutzerkontos nicht erfolgreich auf ein anderes Google Workspace Benutzerkonto übertragen. Der Transfer scheitert an den Nutzerdaten der Applikation Rocket. Workaround: Hinterlegen Sie in den erweiterten Einstellungen der Systemverbindung zur Google Workspace ein Nutzerdatentransfer 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. Ausführliche Informationen und ein Beispiel-XML finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Google Workspace-Umgebung*.	33104
Wenn in der Schematypdefinition einer Schemaerweiterungsdatei für das SAP R/3-Schema ein `DisplayPattern` definiert ist und darin Spalten verwendet werden, die im SAP R/3-Schema einen anderen Namen haben als im One Identity Manager Schema, können Performanceprobleme auftreten. Lösung: Lassen Sie `DisplayPattern` in der Schematypdefinition leer. Es wird automatisch der definierte Name des Objekts als Anzeigewert verwendet.	33812
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. Lösung: Nachgestellte Leerzeichen sollten bereits im Zielsystem vermieden werden.	33448
Der Prozess zur Provisionierung von Objektänderungen startet, bevor das Synchronisationsprojekt aktualisiert wurde.	

Bekanntes Problem	Fehler ID
Lösung: Reaktivieren Sie den Prozess zur Provisionierung von Objektänderungen, nachdem der Prozess `DPR_Migrate_Shell` abgearbeitet wurde.	
Nach einem Update von SAP_BASIS 7.40 SP 0023 auf SP 0026 oder SAP_BASIS 7.50 SP 0019 auf SP 0022 kann sich der SAP R/3 Konnektor nicht mehr mit dem Zielsystem verbinden.	34650

Tabelle 12: Identity Management und Access Governance

Bekanntes Problem	Fehler ID
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.	31997
Wenn eine Zuweisung über die Rollenhierarchie vererbt wird, wird an der geerbten Zuweisung das **Bit 1** gesetzt. Geerbte Zuweisungen sind folglich immer indirekt zugewiesen, auch wenn sie ursprünglich direkt, über eine dynamische Rolle oder eine Zuweisungsbestellung entstanden sind.	35193

Tabelle 13: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
Die Installation des One Identity Manager Service mit Server Installer auf einem Windows Server funktioniert nicht, wenn die Einstellung **File and Printer Sharing** am Server deaktiviert ist. Auf einem Domänen-Controller ist diese Einstellung aus Sicherheitsgründen deaktiviert.	24784
Beim Verbinden mit einer Oracle Database kommt es sporadisch zu einem der folgenden Fehler: TNS-12516, TNS-12519 oder ORA-12520. Erneute Verbindungsversuche sind jedoch meist erfolgreich. Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am Server konfigurierte Limit.	27830
In einem mehrseitigen Synchronisationsprotokoll kann nicht mit der Maus und mit den Pfeiltasten navigiert werden. Ursache: Die StimulReport.Net-Komponente der Firma Stimulsoft behandelt den Bericht als eine Seite.	29051
Gültiger CSS-Code verursacht einen Fehler unter Mono, wenn doppelte Schlüssel vorhanden sind. Weitere Informationen finden Sie unter https://github.com/mono/mono/issues/7455.	762534, 762548, 29607
Mitgliedschaften in Active Directory Gruppen vom Typ **Universal** in einer untergeordneten Domäne werden im Zielsystem nicht entfernt, wenn eines der folgenden Windows Updates installiert ist:	30575

Bekanntes Problem	Fehler ID
• Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 Uns ist derzeit nicht bekannt, ob weitere Windows Updates zu diesem Fehler führen können. Der Active Directory Konnektor korrigiert dieses Fehlverhalten mit einem Workaround beim Aktualisieren der Mitgliederliste. Da dieser Workaround die Performance bei der Provisionierung von Active Directory Gruppen verschlechtern kann, wird er aus künftigen One Identity Manager Versionen wieder entfernt, sobald Microsoft diesen Fehler behoben hat.	
Unter Umständen kommt es im Report Editor zur Verwendung der falschen Sprache in den Steuerelementen von Stimulsoft.	31155
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:
 	
`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 `PowershellCompomentNet4` über einen benutzerdefinierten Windows PowerShell-Aufruf setzen lassen.
	33026

Schemaänderungen

Nachfolgend finden Sie eine Übersicht der Schemaänderungen von Version 8.2.1 zu Version 9.0.

OneLogin Modul

- Neues Datenmodell für das OneLogin Modul.

Konfigurationsmodul

- Neue Spalten `DialogHistoryDB.IsTransportTarget` und `DialogHistoryDB.TransportConnectionString` für die Archivierung der Daten in eine One Identity Manager History Database.
- Neue Spalte `DialogParameter.OnPropertyChangedScript` zur Abbildung eines Skriptes, das bei Wertänderungen ausgeführt wird.
- Neue Spalte `DialogProcessSubstitute.ReadyForDeleteOrExport` zur Kennzeichnung, ob ein Prozess abgeschlossen ist und gelöscht bzw. exportiert werden kann.
- Neue Spalte `DialogTable.TransportSingleUser` zu Abbildung eines Einzelbenutzermodus für den Transport.
- Neue Spalte `DialogUser.IsDisabledForDirectLogin` zur Kennzeichnung, ob der Systembenutzer für die direkte Anmeldung verwendet werden kann.
- Neue Spalten `QBMFileHasDeployTarget.ObjectKeyDeployTarget` und `QBMFileHasDeployTarget.UID_QBMFileHasDeployTarget` zur Zuweisung von Dateien an Maschinenrollen.
- Neue Spalte `QBMPwdPolicy.AdditionalPwdRequirements` für die Beschreibung der zusätzlichen Anforderungen an das Kennwort, die im Testskript geprüft werden.
- Neue Spalten `QBMServer.IsJobServiceSuspended` und `QBMServer.SuspendReason` zur Stoppen des Dienstes während des Offline-Modus eines Zielsystems.
- Neue Pflichtfelddefinition für die Spalte `QBMFileHasDeployTarget.XObjectKey`.
- Die folgenden Spalten wurden auf `varchar(990)` verlängert.
    - DialogHistoryDB.ConnectionString
    - DialogWebService.ProxyPassword
    - DialogWebService.UserPassword
    - QBMPwdPolicy.DefaultInitialPassword
    - QBMServer.SRVAccount
    - QBMServer.SRVAccountDomain
    - QBMServer.SRVAccountPwd
- Die Spalten `QBMVPwdPolicyColumns.ColumnName` und `QBMVPwdPolicyColumns.TableName` wurden auf `varchar(30)` verlängert.

- Die Spalten QBMVPwdPolicyColumns.UID_DialogColumn und QBMVPwdPolicyColumns.UID_DialogTableReference wurden auf varchar(38) verlängert.
- Die Spalte QBMFileHasDeployTarget.UID_QBMDeployTarget wurde gelöscht.

Modul Zielsystemsynchronisation

- Neue Spalte DialogColumn.SyncInfo zur Abbildung von Einschränkungen für die Synchronisation von Spalten.
- Neue Spalte DPRAttachedDataStore.OwnerSchema zur besseren Zugriff auf Schemainformationen.
- Neue Spalten DPRJournal.CausingEntityDisplay, DPRJournal.CausingEntityKey und DPRJournal.JobId zur verbesserten Protokollierung.
- Neue Spalte DPRProjectionStartInfo.CurrentJobReference zur Abbildung des aktuell laufenden Prozesses.
- Neue Spalten DPRRootObjConnectionInfo.IsOffline und DPRRootObjConnectionInfo.IsOfflineModeAvailable zur Kennzeichnung des Offline-Modus.
- Der Datentyp der Spalte DPRShell.IsFinalized wurde auf int geändert.

Zielsystem Basismodul

- Neue Tabelle TSBSpecificGroupBehavior zum Überschreiben der Vererbungseinstellungen für Gruppen aus dem Automatisierungsgrad.
- Die Spalte UNSAccountB.Password wurde auf varchar(990) verlängert.

Azure Active Directory Modul

- Neue Tabellen AADAdministrativeUnit, AADGroupInAdministrativeUnit und AADUserInAdministrativeUnit zur Abbildung von Azure Active Directory Verwaltungseinheiten.
- Neue Tabelle AADUserIdentity und neue Spalte AADUser.Identities zur Abbildung von Identitäten für Azure Active Directory Benutzerkonten.
- Neue Tabelle AADGroupInDirectoryRole und neue Spalte AADGroup.IsAssignableToRole für die Zuweisung von Azure Active Directory Gruppen an Administratorrollen.
- Neue Tabelle AADGroupClassificationLbl zur Klassifizierung von Office 365 Gruppen.
- Neue Spalte AADOrganization.TenantType zur Abbildung von Mandantentypen.
- Neue Spalte AADUser.CreationType zur Abbildung des Erstellungstyps für Azure Active Directory Benutzerkonten.
- Neue Spalten AADGroup.MembershipProcessingState und AADGroup.MembershipRule zur Abbildung von Regeln für Mitgliedschaften in dynamischen Azure Active Directory Gruppen.
- Die Spalte AADUser.Password wurde auf varchar(990) verlängert.

Exchange Online Modul

- Neue Tabellen `O3EMailboxFullAccessPerm` und `O3EMailboxSendAsPerm` zur Abbildungen von Postfachberechtigungen.
- Neue Spalten `O3EMailbox.IssueWarningQuota`, `O3EMailbox.ProhibitSendQuota` und `O3EMailbox.ProhibitSendReceiveQuota` zur Abbildung von Grenzwerten für Exchange Online Postfächer.
- Neue Spalte `O3EUnifiedGroup.UID_AADGroupClassificationLbl` zur Klassifizierung von Office 365 Gruppen.
- Die Spalte `O3EMailUser.Password` wurde auf `varchar(990)` verlängert.

Active Directory Modul

- Neue Spalten `ADSDomain.AdUserName`, `ADSDomain.AdUserPassword` und `ADSDomain.UID_ADSMachineRIDMaster` zur Unterstützung des Verschiebens von Active Directory Objekten über Domänengrenzen hinweg.
- Die Spalte `ADSAccount.UserPassword` wurde auf `varchar(990)` verlängert.

Microsoft Exchange Modul

- Neue Spalten `EX0DL.RecipientType` und `EX0DL.RecipientTypeDetails` zur Abbildung von Empfängertypen für E-Mail aktivierte Verteilergruppen.
- Die Spalte `ADSDomain.EX0UserPassword` wurde auf `varchar(990)` verlängert.

LDAP Modul

- Die Spalten `LDAPAccount.UserPassword` und `LDAPContainer.UserPassword` wurden auf `varchar(990)` verlängert.

Oracle E-Business Suite Modul

- Die Spalte `EBSUser.Password` wurde auf `varchar(990)` verlängert.

Domino Modul

- Die folgenden Spalten wurden auf `varchar(990)` verlängert.
  - NDOCertifier.Password
  - NDOServer.Password
  - NDOUser.InternetPassword
  - NDOUser.Password
  - NDOUser.PasswordInitial

Google Workspace Modul

- Neue Tabellen `GAPExternalEmail` und `GAPExternalEmailInGroup` zur Abbildung externer E-Mail-Adressen.
- Die Spalte `GAPUser.Password` wurde auf `varchar(990)` verlängert.

SAP R/3 Benutzermanagement-Modul

- Neue Spalte `ESetHasEntitlement.ParameterValue` zur Vererbung von SAP Parametern an Systemrollen.
- Neue Spalte `SAPVSAPUserInSAPRoleAll.UID_SAPMandant` zur verbesserten Anzeige von Anzeige von Rollen, Gruppen und Profilen für SAP R/3 Benutzerkonten.
- Die Spalte `SAPUser.Password` wurde auf `varchar(990)` verlängert.

Privileged Account Governance Modul

- Neue Spalten zur Abbildung von Zugriffsanforderungen für Remote-Desktop-Sitzungsanforderung für One Identity Safeguard.
  - PAGAsset.IsRDPApplicationHostPlatform
  - PAGReqPolicy.ObjectKeyRDPAppHostAccount
  - PAGReqPolicy.RDPApplicationAlias
  - PAGReqPolicy.RDPApplicationDisplayName
  - PAGReqPolicy.UID_PAGAssetRDPAppHost
- Neue Spalten zur Abbildung für Zugriffsanforderungen für SSH-Schlüssel für One Identity Safeguard.
  - PAGAsset.SSHHostKeyFingerPrintSha256
  - PAGReqPolicy.AllowSessionSSHKeyRelease
  - PAGReqPolicy.ChangeSSHKeyAfterCheckin
  - PAGReqPolicy.PassphraseProtectSSHKey
- Neue Spalte `PAGUser.ChangePasswordAtNextLogin` zur Kennzeichnung, ob der Benutzer das Kennwort bei der nächsten Anmeldung ändern muss.
- Neue Spalte `PAGUsrGroup.AdminRoles` zur Abbildung einer Liste der Berechtigungen, die alle der Gruppe hinzugefügten Benutzer erhalten sollen.
- Neue Spalte `PAGUsrGroup.AllowPersonalAccounts` zur Unterstützung des Vault für persönliche Kennwörter.
- Die Spalte `PAGUser.Password` wurde auf `varchar(990)` verlängert.

Modul Cloud Systems Management

- Die Spalte `CSMUser.Password` wurde auf `varchar(990)` verlängert.

Modul Universal Cloud Interface

- Die Spalte `UCIUser.Password` wurde auf `varchar(990)` verlängert.

Identity Management Basismodul

- Neue Tabelle `QERTermsOfUseHasFile` zum Zuweisen von Dateien zu Nutzungsbedingungen.
- Neue Spalte `AccProduct.IsToHideFromITShop` zur Kennzeichnung, ob die Leistungsposition aus dem Servicekatalog ausgeblendet wird.
- Neue Spalten `PersonWantsOrg.Recommendation` und `PersonWantsOrg.RecommendationDetail` zur Abbildung von Entscheidungsempfehlungen für den Genehmiger im IT Shop.
- Neue Spalte `PersonWantsOrg.ObjectKeyFinal` zur Abbilung des effektiv zugewiesenen Produktes.
- Neue Spalten `PersonWantsOrg.UID_QERJustificationOrder` und `ShoppingCartItem.UID_QERJustificationOrder` zur Abbildung von Standardbegründungen.
- Neue Spalte `PWODecisionMethod.IsHideFromSelection` zur Kennzeichnung, ob die Entscheidungsrichtlinie im Web Portal ausgeblendet werden soll.
- Die Spalten `Person.CentralPassword` und `Person.Passcode` wurden auf `varchar(990)` verlängert.
- Die Spalten `PWODecisionStep.ComplianceRelevance` und `QERWorkingStep.ComplianceRelevance` wurden gelöscht.

Modul Attestierung

- Neue Tabelle `AttestationPolicyGroup` und neue Spalten `AttestationPolicy.UID_AttestationPolicyGroup` und `AttestationRun.UID_AttestationPolicyGroup` zur Gruppierung von Attestierungsrichtlinien.
- Neue Spalten `AttestationCase.Recommendation` und `AttestationCase.RecommendationDetail` zur Abbildung von Entscheidungsempfehlungen für den Genehmiger im IT Shop.
- Neue Spalte `AttestationObject.ObjectReportMode` als Snapshot des Attestierungsobjektes.
- Neue Spalten `AttestationPolicy.ApproveReasonType` und `AttestationPolicy.DenyReasonType` zur Abbildung der Art der Begründung.
- Neue Spalte `AttestationPolicy.IsSingleCaseNotification` zur Kennzeichnung, ob Benachrichtigungen über offene Attestierungen immer versendet werden.
- Neue Spalte `AttestationPolicy.UID_QERTermsOfUse` zum Zuweisen von Nutzungsbedingungen.
- Neue Spalte `AttestationRun.UID_AttestationPolicy` zur Abbildung der Attestierungsrichtlinie.

Application Governance Modul

- Neue Spalten `AOBApplication.WhereClause` und `AOBApplication.WhereClauseAddOn` zur Definition von Filterbedingungen für die automatische Erzeugung von Anwendungsberechtigungen.
- Neue Spalte `AOBEntitlement.IsDynamic` zur Kennzeichnung von automatisch erzeugten Anwendungsberechtigungen.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 8.2.1 zu Version 9.0. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 64.

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 37.

Tabelle 14: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Modul Zielsys-temsynchronisation	Automatic One Identity Manager Synchronization	geändert
Azure Active Directory Modul	Azure Active Directory Synchronization	geändert
	Azure Active Directory B2C tenant	neu
Active Directory Modul	Active Directory Synchronization	geändert
Active Roles Modul	Synchronize Active Directory Domain via Active Roles	keine
Modul Cloud Systems Management	Universal Cloud Interface Synchronization	geändert
Oracle E-Business Suite Modul	Oracle E-Business Suite Synchronization	geändert
	Oracle E-Business Suite CRM data	geändert

Modul	Synchronisationsvorlage	Art der Änderung
	Oracle E-Business Suite HR data	geändert
	Oracle E-Business Suite OIM data	geändert
Microsoft Exchange Modul	Microsoft Exchange 2013/2016/2019 Synchronization (v2)	geändert
	Microsoft Exchange 2013 / 2016 Synchronization (abgekündigt)	gelöscht
	Microsoft Exchange 2010 Synchronization (v2)	gelöscht
Google Workspace Modul	Google Workspace Synchronization	geändert
LDAP Modul	AD LDS Synchronization	geändert
	AD LDS Synchronization (version 2)	geändert
	OpenDJ Synchronization	geändert
	OpenDJ Synchronization (version 2)	geändert
	Generic LDAP Synchronization (version 2)	geändert
	Oracle DSEE Synchronization (version 2)	geändert
Domino Modul	Lotus Domino Synchronization	geändert
Exchange Online Modul	Exchange Online Synchronization (v2)	geändert
Microsoft Teams Modul	Microsoft Teams (via Azure Active Directory)	geändert
OneLogin Modul	OneLogin Domain Synchronization	neu
Privileged Account Gover-nance Modul	One Identity Safeguard Synchronization	geändert
SAP R/3 Benutzermanagement-Modul	SAP R/3 Synchronization (Base Administration)	geändert
	SAP R/3 (CUA subsystem)	keine
Modul SAP R/3 Analyseberechtigungen Add-on	SAP R/3 BW	keine
Modul SAP R/3 Compliance Add-on	SAP R/3 authorization objects	keine
Modul SAP R/3 Strukturelle Profile Add-on	SAP R/3 HCM authentication objects	geändert
	SAP R/3 HCM employee objects	geändert

Modul	Synchronisationsvorlage	Art der Änderung
SharePoint Modul	SharePoint Synchronization	keine
SharePoint Online Modul	SharePoint Online Synchronization	geändert
Modul Universal Cloud Interface	SCIM Connect via One Identity Starling Connect	geändert
	SCIM Synchronization	geändert
Modul Unix-basierte Zielsysteme	Unix Account Management	keine
	AIX Account Management	keine

Patches für Synchronisationsprojekte

Im One Identity Manager 9.0 werden Patches für folgende Patchtypen bereitgestellt:

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

Um bestehende Synchronisationsprojekte an die One Identity Manager Version 9.0 anzupassen, müssen die Meilensteine angewendet werden. Je Kontext wird ein Meilenstein bereitgestellt. Ein Meilenstein fasst alle Patches für gelöste Probleme und die Meilensteine der Vorversionen zusammen, wenn diese noch nicht angewendet wurden. Sobald der aktuelle Meilenstein auf ein Synchronisationsprojekt angewendet wurde, ist dieses Synchronisationsprojekt mit dem One Identity Manager 9.0 kompatibel.

Patches für neue Funktionen können optional angewendet werden.

Nachfolgend finden Sie eine Liste der Patches für Synchronisationsprojekte, die im One Identity Manager 9.0 neu bereitgestellt werden. Es sind nur die Patches aufgelistet, die nach der Version 8.2.1 neu erstellt wurden. Einen Überblick über die Patches früherer One Identity Manager Versionen erhalten Sie in den jeweiligen Versionsinformationen für diese Versionen.

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

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

Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 64.

Tabelle 15: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **DPR**.	
	Meilenstein 9.0	Meilenstein für den Kontext **One Identity Manager**.	

Tabelle 16: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33400	Neue Property-Mapping-Regel für die Zuweisung von Administratorrollen an Azure Active Directory Gruppen	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `IsAssignableToRole` in das Mapping `Group` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. Abhängig von Patch **Filtert die Mitglieder von Administratorrollen** (VPR#33399).	33400
VPR#34744	Neue Property-Mapping-Regeln für die Abbildung von Eigenschaften dynamischer Azure Active Directory Gruppen	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `membershipRuleProcessingState` und `membershipRule` in das Mapping `Group` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34744
VPR#35033	Unterstützung von B2C Mandanten	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `TenantType` und `Identities` in die Mappings `Organization` und `User` ein.	35033
VPR#35286	Ermöglicht das Schreiben der E-Mail-Adresse von Azure Active Directory Benutzerkonten	Ändert die Property-Mapping-Regel für die Schemaeigenschaft `Mail` im Mapping `User`. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35286

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35289	Unterstützung von Verwaltungseinheiten	Erweitert die Synchronisationskonfiguration zur Unterstützung von Verwaltungseinheiten. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35289
VPR#35290	Neue Property-Mapping-Regel für den Erstellungstyp von Azure Active Directory Benutzerkonten	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `CreationType` in das Mapping `User` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35290
VPR#35303_AAD	Unterstützung von Klassifizierungen	Erweitert die Synchronisationskonfiguration zur Unterstützung der Klassifizierung von Exchange Online Office 365 Gruppen.	35303
VPR#35768	Korrektur des Mappings `ServicePrincipal`	Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft `Owners` im Mapping `ServicePrincipal`. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. Abhängig von Patch **Unterstützung für Azure Active Directory Dienstprinzipale** (VPR#33088).	35768
	Meilenstein 9.0	Meilenstein für den Kontext **Azure Active Directory**.	

Tabelle 17: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35533	Entfernen ungenutzter Schemaeigenschaften	Entfernt ungenutzte virtuelle Schemaeigenschaften aus dem Mapping `site`.	35533

Patch ID	Patch	Beschreibung	Fehler ID
		Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
VPR#33793	Neue Property-Mapping-Regel für die Abbildung des RID-Master der Domäne	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `UID_ADSMachineRIDMaster` in das Mapping `domainDNS` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	33793
	Meilenstein 9.0	Meilenstein für den Kontext **Active Directory**.	

Tabelle 18: Patches für Active Roles

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35122	Aktualisierung des Zielsystemschemas	Aktualisiert das Zielsystemschema, um Datentypen im gespeicherten Schema zu aktualisieren. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35122
	Meilenstein 9.0	Meilenstein für den Kontext **Active Roles**.	

Tabelle 19: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31374	Unterstützung von Raumlisten	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `RecipientType` und `RecipientTypeDetails` in das Mapping `DistributionGroup` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	31374
VPR#35506	Korrigiert das Verhalten von "unbegrenzten" Werten	Die Behandlung von "unbegrenzten" Werten wird korrigiert. Dafür werden Schemaeigenschaften und Property-Mapping-Regeln angepasst.	35506

Patch ID	Patch	Beschreibung	Fehler ID
		Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 9.0	Meilenstein für den Kontext **Microsoft Exchange**.	

Tabelle 20: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30841	Verhindert das Anlegen weiterer Basisobjekte	Ändert die Einstellungen von Synchronisationsprojekten, um das Anlegen von mehr als einem Basisobjekt zu verhindern. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	30841
VPR#34568	Neue Property-Mapping-Regeln für die Abbildung von Quota-Einstellungen für Postfächer	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `ProhibitSendQuota`, `IssueWarningQuota` und `ProhibitSendReceiveQuota` in das Mapping `Mailbox` ein.	34568
VPR#34265	Unterstützung von Postfachberechtigungen	Erweitert die Synchronisationskonfiguration zur Abbildung der Postfachberechtigungen **Vollzugriff** und **Senden als**. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34265
VPR#34766	Unterstützung zertifikatsbasierter Authentifizierung	Legt die Variable `AADOrganization` im Standardvariablenset an. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34766
VPR#35303_O3E	Unterstützung von Klassifizierungen	Erweitert die Synchronisationskonfiguration	35303

Patch ID	Patch	Beschreibung	Fehler ID
		zur Unterstützung der Klassifizierung von Exchange Online Office 365 Gruppen. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 9.0	Meilenstein für den Kontext **Exchange Online**.	

Tabelle 21: Patches für Microsoft Teams

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35410	Aktualisierung des One Identity Manager Schemas	Aktualisiert das One Identity Manager Schema, um den Scope für `O3TTeam` und `O3TTeamChannel` richtig zu setzen. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35410
	Meilenstein 9.0	Meilenstein für den Kontext **Azure Active Directory**.	

Tabelle 22: Patches für Google Workspace

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34885	Erweiterungen für die Synchronisation von Google Workspace externen E-Mail-Adressen	Erweitert die Synchronisationskonfiguration zur Synchronisation von externen E-Mail-Adressen.	34885
	Meilenstein 9.0	Meilenstein für den Kontext **Google Workspace**.	

Tabelle 23: Patches für LDAP

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35702	Ignorieren von Groß- und Kleinschreibung beim Wertevergleich	Aktiviert die Option **Groß-/Kleinschreibung ignorieren** in Property-Mapping-Regeln für die Schemaeigenschaften `ObjectClass` und `StructuralObjectClass`. Dieser Patch wird während der Aktua-	35702

Patch ID	Patch	Beschreibung	Fehler ID
		lisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 9.0	Meilenstein für den Kontext **LDAP**.	

Tabelle 24: Patches für HCL Domino

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35500	Korrektur der Schemaeigenschaft `vrtProxyDataBaseName`	Korrigiert das Skript zum Lesen der Schemaeigenschaft `vrtProxyDataBaseName` der Schemaklasse `AdminRequest (all)`. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35500
VPR#35745	Prüft den Wert der Variable `MailFileAccessType`	Prüft und korrigiert die Variable `MailFileAccessType` in allen Variablensets. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35745
	Meilenstein 9.0	Meilenstein für den Kontext **HCL Domino**.	

Tabelle 25: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35621	Unterstützung für One Identity Safeguard 7.0 (LTS)	Erweitert die Synchronisationskonfiguration zur Unterstützung der Version 7.0 (LTS) von One Identity Safeguard.	35621
	Meilenstein 9.0	Meilenstein für den Kontext **Privileged Account Management**.	

Tabelle 26: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34646_SAP	Aktualisierung des Zielsystemschemas	Aktualisiert das Zielsystemschema.	34646

Patch ID	Patch	Beschreibung	Fehler ID
		Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 9.0	Meilenstein für den Kontext **SAP R/3**.	

Tabelle 27: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32154	Aktivierung der Revisionsfilterung	Aktiviert die Revisionsfilterung in den Synchronisationsschritten **Main Identity**, **Workdates of Employee** und **Communication Data**.	32154
	Meilenstein 9.0	Meilenstein für den Kontext **SAP R/3 Strukturelle Profile Add-on**.	

Tabelle 28: Patches für SAP R/3 BI Analyseberechtigungen

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **SAP R/3 Analyseberechtigungen Add-on**.	

Tabelle 29: Patches für SAP R/3 Berechtigungsobjekte

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **SAP R/3**.	

Tabelle 30: Patches für SharePoint

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **SharePoint**.	

Tabelle 31: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#30841	Verhindert das Anlegen weiterer Basisobjekte	Ändert die Einstellungen von Synchronisationsprojekten, um das Anlegen von mehr als einem Basisobjekt zu verhindern. Dieser Patch wird während der Aktualisierung des One Identity Manager	30841

Patch ID	Patch	Beschreibung	Fehler ID
		automatisch angewendet.	
	Meilenstein 9.0	Meilenstein für den Kontext **SharePoint Online**.	

Tabelle 32: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34952	Zusätzliche Zertifikatsoptionen für Systemverbindungen	Fügt neue Variablen ins Standardvariablenset und die Verbindungsparameter ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34952
VPR#35571	Neue Variable zur Konfiguration eines Request Timeout	Fügt eine Variable zur Konfiguration des Request Timeout ins Standardvariablenset und die Verbindungsparameter ein.	35571
	Meilenstein 9.0	Meilenstein für den Kontext **SCIM**.	

Tabelle 33: Patches für die Universal Cloud Interface-Schnittstelle (im Modul Cloud Systems Management)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35451	Behandlung der `XIsInEffect`-Spalten für alle `UserInGroup*` und `UserHasGroup*` Tabellen	Fügt die Spezialbehandlung der `XIsInEffect`-Spalten für alle `UserInGroup*` und `UserHasGroup*` Tabellen in die entsprechenden Mappings und Workflows ein.	35451
	Meilenstein 9.0	Meilenstein für den Kontext **Universal Cloud Interface**.	

Tabelle 34: Patches für Unix

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **Unix**.	

Tabelle 35: Patches für den One Identity Manager Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **Datenbank**.	

Tabelle 36: Patches für den CSV-Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.0	Meilenstein für den Kontext **CSV**.	

Abgekündigte Funktionen

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

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

  Verwenden Sie das Kennwortrücksetzungsportal um Kennwörter zu ändern. Kennwortfragen und Kennwortantworten hinterlegen Sie im Web Portal.
- Der SOAP Web Service wird nicht mehr unterstützt.
- Der SPML Webservice wird nicht mehr unterstützt.
- Der API Designer wird nicht mehr unterstützt.

  Im One Identity Manager API-Entwicklungshandbuch wurde eine Anleitung hinzugefügt, wie man XML-basierten API-Definitionscode in eine Plugin-Bibliothek umwandelt.
- Die Verwaltung verschiedener Versionen eines kompilierten Projektes mithilfe von Kompilierungszweigen wird nicht mehr unterstützt.
- Die Visual Studio Code-Erweiterung für die HTML-Anwendungsentwicklung wird nicht mehr unterstützt.
- Die Kompilierung von HTML-Anwendungen im Database Compiler wird nicht mehr unterstützt.
- Der SharePoint 2010 Konnektor wird nicht mehr unterstützt.
- Der Microsoft Exchange 2010 Konnektor wird nicht mehr unterstützt.
- Die Eigenschaft **Relevanz für Compliance** für IT Shop Bestellungen (`PWODecisionStep.ComplianceRelevance` und `QERWorkingStep.ComplianceRelevance`) wird nicht mehr unterstützt.
- Starling Two-Factor Authentication und die Starling 2FA App werden nicht mehr unterstützt, da der Dienst Starling Two-Factor Authentication zum 1. November 2022 abgeschaltet wird.

    - Für die Multifaktor-Authentifizierung bei Bestellungen oder Attestierungen wird OneLogin genutzt.
    - Für die Entscheidung von Bestellungen und Attestierungsvorgängen nutzen Sie die neue Funktionalität der adaptiven Karten mit Starling Cloud Assistant.
- Der generische LDAP Konnektor wird nicht mehr unterstützt. Verwenden Sie den **LDAP Konnektor (Version 2)**.

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

- Folgende Skripte sind als veraltet gekennzeichnet. Bei der Kompilierung wird eine entsprechende Warnung ausgegeben.
    - VI_GetValueOfObject
    - VID_GetValueOfDialogObject
    - VI_ITDataFromOrg
    - VI_AE_ITDataFromOrg
    - VI_GetOrgUnitFromCertifier
    - VI_ConvertDNToCanonicalName
    - VI_PersonAuto_LDAP
    - VI_PersonAuto_ADS
    - VI_PersonAuto_EBS
    - VI_PersonAuto_Notes
    - VI_PersonAuto_SAP
    - VI_PersonAuto_SharePoint_SPSUser
    - VI_GetAttestationObject

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*.

> HINWEIS: Beim Einrichten einer virtuellen Umgebung sollten Sie die Konfigurationsaspekte wie CPU, Speicherverfügbarkeit, I/O-Subsystem und Netzwerkinfrastruktur sorgfältig berücksichtigen, um sicherzustellen, dass die virtuelle Schicht über die erforderlichen Ressourcen verfügt. Weitere Informationen zur Umgebungsvirtualisierung finden Sie in den Richtlinien für den Produktsupport.

Jede One Identity Manager Installation kann virtualisiert werden. Stellen Sie sicher, dass der jeweiligen One Identity Manager-Komponente die laut Systemanforderung spezifizierte Leistung und Ressourcen zur Verfügung stehen. Idealerweise sollten Ressourcenzuordnungen für den Datenbankserver statisch festgesetzt werden. Die

Virtualisierung einer One Identity Manager Installation sollte von Experten mit einem fundierten Wissen über Virtualisierungstechniken vorgenommen werden.

Unterstützte Datenbanksysteme

One Identity Manager unterstützt folgende Datenbanksysteme:

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

Minimalanforderungen für den Einsatz von SQL Server als Datenbankserver

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

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung (nicht-produktiv) 16 physische Kerne mit 2.5 GHz+ Taktung (produktiv) HINWEIS: Aus Performancegründen wird der Einsatz von 16 physischen Kernen empfohlen.
Arbeitsspeicher	16 GB+ RAM (nicht-produktiv) 64 GB+ RAM (produktiv)
Freier Festplattenspeicher	100 GB
Betriebssystem	Windows Betriebssysteme • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. UNIX und Linux Betriebssysteme • Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.
Software	Unterstützt werden die Versionen: • SQL Server 2019 Standard Edition (64-Bit) mit aktuellem

kumulativen Update

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

HINWEIS: Aus Performancegründen wird für produktive Systeme der Einsatz der SQL Server Enterprise Edition empfohlen.

- Kompatibilitätsgrad für Datenbanken: SQL Server 2019 (150)
- Standard-Sortierschema: Case-Insensitiv, SQL_Latin1_General_CP1_CI_AS (Empfehlung)
- SQL Server Management Studio (empfohlen)

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

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

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

Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank

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

Minimalanforderungen für Clients

Auf den Clients sind die folgenden Systemvoraussetzungen zu gewährleisten.

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

Minimalanforderungen für Jobserver

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

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	16 GB RAM
Freier Festplat-tenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016

	• Windows Server 2012 R2 • Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden.
Zusätzliche Software	Windows Betriebssysteme • Microsoft .NET Framework Version 4.8 oder höher HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers. Linux Betriebssysteme • Mono 5.14 oder höher

Minimalanforderungen für Webserver

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

Prozessor	4 physische Kerne mit 1.65 GHz+Taktung
Arbeitsspeicher	4 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden. Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für Apache HTTP Server.

Zusätzliche Software	Windows Betriebssysteme
	• Microsoft .NET Framework Version 4.8 oder höher
	• Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.8 und den Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions
	  • Web Server > Application Development > ISAPI Filters
	  • Web Server > Security > Basic Authentication
	  • Web Server > Security > Windows Authentication
	  • Web Server > Performance > Static Content Compression
	  • Web Server > Performance > Dynamic Content Compression
	Linux Betriebssysteme
	• NTP - Client
	• Mono 5.14 oder höher
	• Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
	  • mod_mono
	  • rewrite
	  • ssl (optional)

Minimalanforderungen für Anwendungsserver

Zur Installation des Anwendungsservers sind die folgenden Systemvoraussetzungen zu gewährleisten.

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

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

- Web Server > Application Development > ISAPI Filters
- Web Server > Security > Basic Authentication
- Web Server > Security > Windows Authentication
- Web Server > Performance > Static Content Compression
- Web Server > Performance > Dynamic Content Compression

Linux Betriebssysteme

- NTP - Client
- Mono 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 37: 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 (Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names) und RFC 4512 (Lightweight Directory Access Protocol (LDAP): Directory

Konnektor	Unterstützte Datensysteme
	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, 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, Windows Server 2019 und Windows Server 2022 ausgeliefert wird.
Microsoft Exchange Konnektor	• Microsoft Exchange 2013 mit kumulativem Update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 mit kumulativem Update 1 • Microsoft Exchange Hybrid-Umgebungen
SharePoint Konnektor	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
SAP R/3 Konnektor	• 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, 7.54 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 One Identity Safeguard Authentication Services.
Domino Konnektor	• IBM Domino Server Version 8, 9 und 10 • HCL Domino Server Version 11 und 12 • IBM Notes Client 8.5.3 und 10.0 • HCL Notes Client Version 11.0.1 und 12.0

Konnektor	Unterstützte Datensysteme
	Die 64-Bit-Variante des Notes Client 12.0.1 wird derzeit nicht unterstützt.
Generischer Datenbankkonnektor	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe Konnektoren	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell Konnektor	• Windows PowerShell Version 3 oder höher
Active Roles Konnektor	• Active Roles 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.5, 7.5.2, 7.5.3 und 7.6
Azure Active Directory Konnektor	• Microsoft Azure Active Directory HINWEIS: Die Synchronisation von Azure Active Directory Mandanten in nationalen Cloud-bereitstellungen mit dem Azure Active Directory Konnektor wird nicht unterstützt. Dies betrifft: • Microsoft Cloud for US Government (L5) • Microsoft Cloud Germany • Azure Active Directory und Microsoft 365 betrieben von 21Vianet in China Weitere Informationen finden Sie auch unter https://-support.oneidentity.com/KB/312379. • Microsoft Teams
SCIM Konnektor	Unterstützt werden Cloud-Anwendungen, welche die System for Cross-domain Identity Management (SCIM) Spezifikation in der Version 2.0 verstehen. Die Anforderungen von RFC 7643 (System for Cross-domain Identity Management: Core Schema)

Konnektor	Unterstützte Datensysteme
	und RFC 7644 (System for Cross-domain Identity Management: Protocol) sind zu gewährleisten.
Exchange Online Konnektor	• Microsoft Exchange Online
Google Workspace Konnektor	• Google Workspace
Oracle E-Business Suite Konnektor	• Oracle E-Business Suite Version 12.1, 12.2 und 12.2.10
SharePoint Online Konnektor	• Microsoft SharePoint Online
One Identity Safeguard Konnektor	• One Identity Safeguard Version 6.0, 6.7, 6.13 und 7.0

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 9.0 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

- One Identity Manager 9.0 ist eine Weiterentwicklung der Version 8.2.1. Alle offiziellen Releases der Versionen 8.2.1, 8.1.5 oder älter sind geeignet für die

Aktualisierung auf Version 9.0. Die Aktualisierung neuerer Versionen kann zu einem Downgrade führen.

- Bevor Sie ein Migrationspaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung. Verwenden Sie eine Kopie der produktiven Datenbank für die Tests.
- Stellen Sie vor der Aktualisierung der One Identity Manager-Datenbank auf die Version 9.0 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 eine One Identity Manager-Datenbank auf einem SQL Server wird aus Performancegründen empfohlen, für die Zeit der Schemaaktualisierung die Datenbank auf das Wiederherstellungsmodell **Einfach** zu setzen.
- Während der Aktualisierung einer One Identity Manager-Datenbank der Version 8.0.x auf die Version 9.0 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\MSSQL2K\30374.sql`). Im Fehlerfall korrigieren Sie die Daten und starten Sie die Aktualisierung erneut.
- 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 Confi-

guration Wizard Reparaturmethoden angeboten, um die Datenbankdatei und die Datendateigruppe zu erstellen.

- Während der Aktualisierung werden Berechnungsaufträge in die Datenbank eingestellt. Diese werden durch den DBQueue Prozessor verarbeitet. Abhängig von Datenumfang und Systemperformance kann die Verarbeitung der Berechnungsaufträge einige Zeit dauern.

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

  Stellen Sie daher vor der Aktualisierung der Datenbank sicher, dass Sie ein entsprechendes Verfahren zur Datenarchivierung konfiguriert haben. Ausführliche Informationen zur Archivierung von Daten finden Sie im *One Identity Manager Administrationshandbuch für die Datenarchivierung*.
- Für den Zeitraum der Aktualisierung wird die Datenbank in den Einzelbenutzermodus gesetzt. Beenden Sie alle bestehenden Verbindungen zur Datenbank vor dem Start der Schemaaktualisierung.
- Bei Einsatz einer Datenbankspiegelung kann es zu Problemen bei der Aktivierung des Einzelbenutzermodus kommen.
- Während der Installation einer neuen One Identity Manager-Datenbank mit der Version 9.0 sowie der Aktualisierung einer One Identity Manager-Datenbank von Version 8.0.x auf die Version 9.0 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.

  > HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 9.0 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 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.

- Nach Beenden der Aktualisierung wird die Datenbank automatisch in den Mehrbenutzermodus geschaltet. Sollte dies nicht möglich sein, erhalten Sie eine Meldung, über die Sie die Datenbank manuell in den Mehrbenutzermodus schalten können.
- Mit der Installation dieser Version benötigen Benutzer, die auf die REST API im Anwendungsserver zugreifen sollen, die Programmfunktion **Erlaubt den Zugriff auf die REST API des Anwendungsservers** (`AppServer_API`). Weisen Sie den Benutzern diese Programmfunktion zu. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Aktualisieren des One Identity Manager auf Version 9.0

WICHTIG: Beachten Sie die Hinweise zur Aktualisierung des One Identity Manager auf Seite 57.

Um eine bestehende One Identity Manager Installation auf die Version 9.0 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 Active Directory Edition zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager Active Directory Edition**.

c. Klicken Sie **Installieren**.

   Der Installationsassistent wird gestartet.

d. Folgen Sie den Installationsanweisungen.

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

3. Beenden Sie den One Identity Manager Service auf dem Aktualisierungsserver.
4. Erstellen Sie eine Sicherung der One Identity Manager-Datenbank.
5. Prüfen Sie, ob der Kompatibilitätsgrad der Datenbank auf den Wert **150** eingestellt ist und passen Sie die Wert bei Bedarf an.
6. Führen Sie die Schemaaktualisierung der One Identity Manager-Datenbank aus.
   - Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation 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 Version 8.0.x auf die Version 9.0 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 Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.
7. Aktualisieren Sie den One Identity Manager Service auf dem Aktualisierungsserver.

   a. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.

b. Wechseln Sie auf den Tabreiter **Installation**. Wählen Sie die Edition, die Sie installiert haben.

   - Um eine One Identity Manager Active Directory Edition zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity ManagerActive Directory Edition**.

c. Klicken Sie **Installieren**.

   Der Installationsassistent wird gestartet.

d. Folgen Sie den Installationsanweisungen.

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

8. Prüfen Sie die Anmeldeinformationen des One Identity Manager Service. Geben Sie das zu verwendende Dienstkonto an.
9. Starten Sie den One Identity Manager Service auf dem Aktualisierungsserver.
10. Aktualisieren Sie weitere Installationen auf Arbeitsstationen und Servern.

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

Um Synchronisationsprojekte auf die Version 9.0 zu aktualisieren

1. Wenn Sie Synchronisationsprojekte für die Anbindung von Cloud-Anwendungen im Universal Cloud Interface eingerichtet haben, aktualisieren Sie in diesen Synchronisationsprojekten das Zielsystemschema. 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 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 64.

Um einen Anwendungsserver auf die Version 9.0 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 Designer Web Portal auf die Version 9.0 zu aktualisieren

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

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

Um einen API Server auf die Version 9.0 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 9.0 zu aktualisieren

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

Um die Manager Webanwendung auf die Version 9.0 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. (Optional) Deaktivieren Sie das Synchronisationsprojekt.

HINWEIS: Beim Aktualisieren bestehender Synchronisationsprojekte werden immer die Verbindungsparameter aus dem Standardvariablenset verwendet. Stellen Sie sicher, dass die Variablen im Standardvariablenset 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 Zielsystemschema, bevor Sie die Patches anwenden. Verwenden Sie den Synchronization Editor.

Um Patches anzuwenden

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

   Im Bereich **Details - Installationszusammenfassung** werden alle abhängigen Patches in der Reihenfolge angezeigt, in der sie angewendet werden.
4. Klicken Sie **Ausgewählte Patches anwenden**.
5. Wenn Benutzereingaben angefordert werden, erfassen Sie die benötigten Daten.
6. (Optional) Wählen Sie im Bereich **Verfügbare Patches** die Patches für neue Funktionen aus, die angewendet werden sollen. Mehrfachauswahl ist möglich.

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

a. Klicken Sie **Ausgewählte Patches anwenden**.

b. Wenn Benutzereingaben angefordert werden, erfassen Sie die benötigten Daten.

7. Prüfen Sie anhand des Patchprotokolls, ob kundenspezifische Anpassungen nachbearbeitet werden müssen.
8. Falls erforderlich, überarbeiten Sie die kundenspezifischen Anpassungen in der Synchronisationskonfiguration.
9. Führen Sie eine Konsistenzprüfung durch.
10. Simulieren Sie die Synchronisation.
11. (Optional) Aktivieren Sie das Synchronisationsprojekt.
12. 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 35
- Patches für Synchronisationsprojekte auf Seite 37

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 2022.0007.0029.0000 für alle Module und die Anwendungsversion 9.0 v90-167803 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

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.