One Identity Manager 8.2

Versionshinweise

26. November 2021, 12:12 Uhr

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 8.2 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 8.1.5 aufgeführt.

One Identity Manager 8.2 ist ein Minor Release mit neuen Funktionen und verbessertem Verhalten. Siehe Neue Funktionen auf Seite 2 und Verbesserungen auf Seite 16.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.1.x 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 8.2

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 bereitgestellten Microservices, die die Funktionen Ihrer On-Prem-Lösungen von One Identity erweitern. Wir werden One Identity Starling ständig neue Produkte und Funktionen zur Verfügung stellen. Eine kostenlose Testversion unserer One Identity Starling-Angebote sowie die neuesten Produktfeatures erhalten Sie unter cloud.oneidentity.com.

Neue Funktionen

Neue Funktionen in One Identity Manager 8.2.

Allgemein

- Wir führen in unseren Produkten und in der Dokumentation eine inklusive Terminologie ein und ersetzen im Laufe des Prozesses die nicht-inklusive Terminologie. Änderungen an den Elementen unserer Benutzeroberfläche und Fehlermeldungen werden in der Dokumentation für jede Produktversion berücksichtigt.
- SQL Server 2019 mit dem Kompatibilitätsgrad für Datenbanken **SQL Server 2017 (140)** wird unterstützt.
- Windows Server 2022 wird für Jobserver, Anwendungsserver und Webserver unterstützt.

- Windows 11 wird für Arbeitsstationen unterstützt.
- Neuer Formatierungstyp, um die Eingabe von XSS-Zeichen zu verhindern. Ob die Prüfung erfolgen soll, wird über die neuen Konfigurationsparameter **QBM | XssCheck** und **QBM | XssCheck | Sync** festgelegt.
- Verbesserter Schutz vor potentiell schädlichen SQL Ausführungen. Neue Konfigurationsparameter **QBM | SQLCheck | RiskEvaluation** und **QBM | SQLCheck | SubSelect** zur Risikoabschätzung.
- Ein Verbindungspool für getrennte Sitzungen für Lesen und Schreiben auf verschiedenen Datenbankservern wird unterstützt. Im Verbindungsdialog kann die Eigenschaft **Data Source** eine Pipe (|) getrennte Serverliste enthalten. Dabei ist der erste angegebene Server der primäre Server, über den die Schreibzugriffe laufen. Alle anderen Server sind Read-Only-Kopien, die nur Lesezugriffe erhalten.
- Für Kennwortrichtlinien kann festgelegt werden, wie viele Regeln für Zeichenklassen erfüllt sein müssen, damit ein Kennwort der Kennwortrichtlinie entspricht.
- Erweiterte Konfiguration für OAuth 2.0/OpenID Connect.
  - Die OAuth 2.0/OpenID Connect Konfiguration für Identitätsanbieters kann aus einer Vorlage ermittelt werden. Für den One Identity Redistributable STS (RSTS) wird die Datei mit einer Vorkonfiguration mitgeliefert. Die Datei `RSTS_Template.xml` finden Sie im One Identity Manager Installationsverzeichnis. Die Vorlage kann im Designer verwendet werden.
  - Es kann festgelegt werden, ob eine Prüfung des ID-Tokens stattfindet.
  - Es können die acr-Werte angegeben werden, welche der Autorisierungsserver für die Verarbeitung einer Authentifizierungsanfrage verwenden soll.
  - Es kann der Claim-Typ angegeben werden, der zusätzlich geprüft werden soll.
  - Das Verhalten des Clients nach dem Abmelden von der Anwendung kann konfiguriert werden.
- Die Authentifizierung externer Anwendungen über OAuth 2.0/OpenID Connect wird unterstützt.

  Zur Konfiguration werden die neuen Konfigurationsparameter **QBM | AppServer | AccessTokenAuth** und **QBM | AppServer | AccessTokenAuth | RoleBased** bereitgestellt.
- Fallback für die Anmeldung über die OAuth 2.0/OpenID Connect-Authentifizierungsmodule für die Ermittlung des Benutzers. Wenn für den Claim-Wert keine passende Person gefunden wird, suchen die Authentifizierungsmodule den Claim-Wert in den zulässigen Anmeldungen der Systembenutzer (`DialogUser.AuthentifierLogons`). Gibt es dort einen Eintrag, wird dieser Systembenutzer angemeldet.
- Personen, die als sicherheitsgefährdend eingestuft sind, können sich nicht mehr am One Identity Manager anmelden. Um die Anmeldung zu erlauben, aktivieren Sie den Konfigurationsparameter **QER | Person | AllowLoginWithSecurityIncident**.
- Zur Abbildung von Listen zulässiger Werte wurde eine neue Tabelle `QBMColumnLimitedValue` implementiert. Zur Abbildung von Bitmasken wurde eine

neue Tabelle `QBMColumnBitMaskConfig` implementiert. Die Bearbeitung erfolgt im Designer im Schemaeditor auf dem Tabreiter **Werteigenschaften**. Standardwerte können kundenspezifisch deaktiviert werden.

- Für die Einzelwerte von MVP-Spalten kann festgelegt werden ob die Werte eindeutig sein müssen, ob die Groß-und Kleinschreibung beachtet werden soll oder ob Akzentzeichen geprüft werden sollen. Die Bearbeitung erfolgt im Designer im Schemaeditor auf dem Tabreiter **Werteigenschaften**.
- Für eindeutige Gruppen von Spalten können Meldungstexte für Fehlermeldungen erfasst werden, die statt der Standardfehlermeldung verwendet werden sollen.
- Für vordefinierte Datenbankabfragen kann über den Typ der Abfrage festgelegt werden, ob es sich um ein komplette Abfrage oder um den Where-Klausel Anteil einer SQL-Abfrage handelt.
- Wenn das Format angegeben wird, ist der Zieltyp des Ausdrucks ein `String`. Wird das Format nicht angegeben, ist es der angegebene Datentyp.
- Es kann festgelegt werden, ob ein Jobserver an der Lastverteilung teilnimmt.
- In kundendefinierten Methodendefinitionen kann ein Skript zum bedingten Anzeigen einer Methode verwendet werden. So kann beispielsweise gesteuert werden, dass eine Methode im Manager nur angezeigt wird, wenn eine bestimmte Bedingung erfüllt ist. Das Skript verändert nicht die Berechtigungen eines Benutzers, sondern lediglich das Verhalten beim Laden eines Objektes in den One Identity Manager-Werkzeugen.
- Neue Funktionen für Zeitpläne.
  - Zeitpläne können an einem bestimmten Wochentag in einem bestimmten Monat ausgeführt werden.
  - Es können mehrere Startzeiten pro Tag festgelegt werden.
  - Das Starten von Zeitplänen wird protokolliert.
- Es kann ein Standardland hinterlegt werden, dass bei der Ermittlung von Arbeitszeiten und Feiertagen berücksichtigt wird.
- Erweiterung der $-Notation um optionale Formatangabe: `$<Definition>:<Datentyp> {<Format>}$`
- Einführung einer neuen One Identity Manager Abfragesprache. Die One Identity Manager Abfragesprache (auch One Identity Manager Query Language) kann zum Erstellen von Abfragen oder Where-Klausel-Ausdrücke gegen die One Identity Manager-Objektschicht verwendet werden. Die One Identity Manager Abfragesprache wird beispielsweise für die Kommunikation zwischen Anwendungsserver und Client genutzt. Sie können die One Identity Manager Abfragesprache derzeit im Object Browser im Abfragefenster verwenden. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Unterstützung von kundenspezifischen Konfigurationsdateien für die Protokollierung mittels NLog. In der Datei `globallog.config` sind die Include-Dateien `custom-log-variables.config` und `custom-log-targets.config` definiert. Über die Variable

`logFileLevel` kann der Informationsgrad in einer kundenspezifischen Konfigurationsdatei überschrieben werden. Über die Variable `eventLogLevel` kann der Informationsgrad in einer kundenspezifischen Konfigurationsdatei überschrieben werden.

- Mit dem Database Transporter können Transportvorlagen erzeugt werden. Die Transportvorlagen können Sie nutzen, wenn Sie Transportpakete mit dem Database Transporter oder mit dem Kommandozeilenprogramm `DBTransporterCMD.exe` erstellen. Dabei werden die Exportkriterien aus der Transportvorlagendatei geladen.
- Das Kommandozeilenprogramm `DBTransporterCMD.exe` unterstützt den Transport von Synchronisationsprojekten.
- Neue Funktionen im Kommandozeilenprogramm `Quantum.MigratorCmd.exe`.
    - Das Erstellen, Prüfen und Erweitern der SQL Server Anmeldungen wird unterstützt, wenn abgestufte Berechtigungen genutzt werden sollen.
    - Neuer Modus zum Herstellen einer betriebsbereiten Datenbank, nachdem die Datenbank aus einer Sicherung wiederhergestellt wurde.
- Das Kommandozeilenprogramm `DBCompilerCMD.exe` unterstützt die automatische Kompilierung der Datenbank. Die Datenbank wird überwacht und bei Bedarf kompiliert.
- Das Kommandozeilenprogramm `AutoUpdate.exe` unterstützt die automatische Softwareaktualisierung einer Installation des One Identity Manager.
- Die One Identity Manager-Werkzeuge werden im Launchpad in einem neuen Menüeintrag **Programme** angezeigt und können dort gestartet werden.
- Einzelnen Aufgaben im Launchpad sind auch für Benutzer mit rollenbasierten Berechtigungsgruppen verfügbar.
- Zur Konfiguration der Mail-Funktionalitäten im One Identity Manager wird ein E-Mail-Konfigurationsassistent zur Verfügung gestellt. Der Assistent kann im Launchpad und im Designer im Konfigurationsparametereditor ausgeführt werden
- Die Benutzeroberfläche einiger One Identity Manager-Komponenten benötigt Microsoft EdgeWebView2, um bestimmte Inhalte darstellen zu können. Bei der Installation der Komponenten wird Microsoft EdgeWebView2 mit installiert.
- Der Anwendungsserver kann auf einen REST API-Modus beschränkt werden.
- Die automatische Aktualisierung des Anwendungsservers kann in der Datei `web.config` konfiguriert werden. Über das Attribut `mode` kann gesteuert werden, ob die Aktualisierung zeitgesteuert erfolgt oder manuell gestartet werden kann.
- Neuer Konfigurationsparameter **Common | Indexing | DefaultResultLimit** um die maximale Anzahl von Suchergebnissen festzulegen, die bei einer Anfrage zurückgegeben werden.
- Der API Server stellt optional eine SCIM V2.0 Schnittstelle über ein Plugin bereit. Darüber kann auf einen definierten Satz von One Identity Manager-Tabellen lesend und schreibend zugegriffen werden.
- Die Verfügbarkeit eines One Identity Manager Service kann über /alive geprüft werden.

- Neue Einstellung `DirectConnection` zur Konfiguration des One Identity Manager Service für direkte Verbindung zur Zieldatenbank ohne Verfügbarkeitstest.
- Neue Einstellung `DoNotWriteConfigBack` zur Konfiguration des One Identity Manager Service, um Konfiguration nicht zurück in die Datenbank zu schreiben.
- Neue Prozesskomponente SFtpComponent. Die Prozesskomponente kann Dateien per SFTP übertragen.
- Neue Prozessfunktion `CallMethodExclusive` für die Prozesskomponente `HandleObjectComponent` zum exklusiven Aufruf einer Customizermethode.
- Die F1-Hilfe und die One Identity Manager Dokumentation werden im HTML5-Format bereitgestellt. Die One Identity Manager Dokumentation erreichen Sie im Manager über das Menü **Hilfe > Suchen in lokaler Hilfe**.
- Integration der Customizer-Methoden in die Typed-Wrapper-Klassen.
- Stufenweise Vorbereitung der Datenbankaktualisierung. Es werden die verschiedenen Phasen zur Vorbereitung der Datenbankaktualisierung durchlaufen. Durch diese stufenweise Vorbereitung soll sichergestellt werden, dass die Benutzer über die bevorstehende Aktualisierung informiert werden und Prozesse gezielt beendet werden können.

  HINWEIS: Die stufenweise Vorbereitung wird nur bei Aktualisierung von Datenbanken eingesetzt, die mindestens die One Identity Manager Version 8.2 haben.

Web Portal

- Diese One Identity Manager Version beinhaltet grundlegend überarbeitete Webanwendungen auf Basis der HTML5-Technologie. Diese Webanwendungen werden über den API Server bereitgestellt und decken unter anderem folgende Anwendungsbereiche ab:
  - IT Shop Bestellungen und Genehmigungen
  - IT Shop Konfiguration
  - Verwalten von Identitäten, Benutzerkonten, Systemberechtigungen, Unternehmensstrukturen und Systemrollen
  - Application Governance
  - Verwalten von Attestierungsrichtlinien
  - Genehmigungen von Attestierungsvorgängen
  - Verwalten von Kennwörtern
  - Überwachen von Prozessen der Jobqueue

  HINWEIS: Beachten Sie, dass die Webanwendungen, die bisher Bestandteil des Produktes waren, auch weiterhin zur Verfügung stehen. Aus Verständnisgründen wird nun zwischen dem Web Designer Web Portal und dem Web Portal unterschieden.
- Application Governance ist nun Bestandteil des Web Portals. Mit Hilfe der Application Governance Funktionen können Sie schnell und einfach den Onboarding-Prozess für

neue Anwendungen zentral durchführen. Eine erstellte Anwendung vereint alle Berechtigungen, die Benutzer der Anwendung für ihre tägliche Arbeit benötigen. So können Sie Ihrer Anwendung Anwendungsberechtigungen (beispielsweise Systemberechtigungen oder Systemrollen) zuweisen und planen, ab wann diese als bestellbare Produkte im Web Portal zur Verfügung stehen.

- Im Web Portal für Betriebsunterstützung ist es nun möglich, als ausstehend markierte Objekte einzusehen, diese Objekte in der Datenbank zu löschen oder dem Zielsystem wieder hinzufügen. Zusätzlich ist es möglich, den Status dieser Objekte zurückzusetzen, so dass sie nicht mehr als ausstehend markiert sind. Es wird eine neue Anwendungsrolle **Basisrollen | Betriebsunterstützung | Nachbehandlung der Synchronisation** bereitgestellt.
- Es ist nun möglich, im Web Portal für Betriebsunterstützung zu entscheiden, wie mit fehlerhaften Prozessen weiter verfahren werden soll. So können Sie beispielsweise fehlerhafte Prozesse und Prozessschritte erneut ausführen.
- Es ist nun möglich, im Web Portal für Betriebsunterstützung neue Kennwörter für Identitäten zu vergeben.
- Sie können nun im Web Portal Produkte anzeigen und bestellen, die andere Mitarbeiter aus Ihrem Umfeld bereits bestellt haben. Als Manager können Sie zudem Produkte aus der Peer-Gruppe eines Mitarbeiters anzeigen, für den Sie verantwortlich sind.
- Es ist nun möglich, im Web Portal Stichprobendaten zu erstellen, zu bearbeiten und zu löschen. Diese Stichprobendaten können dann in Attestierungsrichtlinien verwendet werden, um Attestierungen nur für eine Teilmenge von Objekten durchzuführen, beispielsweise wenn die Attestierung aller Objekte zu lange dauern würde.
- Im Web Portal kann man nun für jede Identität ein Organigramm anzeigen.
- Im Web Portal gibt es nun auf der Startseite eine Kachel **Bald ablaufende Produkte**, die auf Produkte hinweist, deren Gültigkeit in naher Zukunft abläuft und verlängert werden muss.
- Mitgliedschaften in Objekten, die über dynamische Rollen zustande gekommen sind, können nun im Web Portal ausgeschlossen werden.
- Es ist nun möglich, im Web Portal Shops und zugehörige Regale zu erstellen, zu bearbeiten und zu löschen.
- Mithilfe des Administration-Portals kann man nun seine API-Konfiguration einsehen und bearbeiten.
- Es ist nun möglich, eigene HTML5-Anwendungen als ZIP-Datei bereitzustellen und über den API Server hosten zu lassen.
- Es ist nun möglich, im Web Portal Servicekategorien zu erstellen, zu bearbeiten und zu löschen.

Zielsystemanbindung

- Unterstützung von Microsoft Teams.

  Im One Identity Manager werden die Teams und Kanäle einer Microsoft Teams-Umgebung abgebildet. Die Synchronisation mit der Microsoft Teams-Umgebung übernimmt der Azure Active Directory Konnektor. Mit der Installation des Microsoft Teams Moduls wird die Synchronisationsvorlage für Microsoft Teams bereitgestellt. Der Azure Active Directory Konnektor verwendet die Microsoft Graph-API für den Zugriff auf Microsoft Teams. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Microsoft Teams-Umgebung*.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32454 bereitgestellt.

- Simulation des Property-Mappings für Einzelobjekte

  Im Synchronization Editor können die Ergebnisse von Property-Mapping-Regeln getestet werden. Damit kann insbesondere das Mapping virtueller Schemaeigenschaften überprüft werden. Die Testergebnisse können exportiert und so für den Produktsupport genutzt werden.

- Die nationale Cloudbereitstellung Microsoft Cloud for US Government (L4) wird unterstützt.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#34150 und der Patch ID VPR#34170 bereitgestellt.

- Azure Active Directory Gastbenutzer werden unterstützt. Um die Einladung für Gastbenutzer zu verschicken, sind zusätzlich Anpassungen im Synchronisationsprojekt erforderlich.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#28669 und mit der Patch ID VPR#32665 bereitgestellt.

- Für Azure Active Directory Benutzerkonten werden zusätzliche Eigenschaften für die Abbildung persönlicher Informationen und Informationen zu Verbund-Umgebungen für Azure Active Directory unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31389 bereitgestellt.

- Das Datum der letzten Kennwortänderung für Azure Active Directory Benutzerkonten wird eingelesen.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32975 bereitgestellt.

- Die Lizenzzuweisung an Azure Active Directory Benutzerkonten über Azure Active Directory Gruppen wird unterstützt. Es werden zusätzliche Berichte für Benutzerkonten und Abonnements bereitgestellt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32384 bereitgestellt.

- Azure Active Directory Anwendungen, Dienstprinzipale und App-Rollen werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33088 bereitgestellt.
- Azure Active Directory Richtlinien zum Inaktivitätstimeout, Richtlinien zur Startbereichsermittlung, Richtlinien zur Token-Ausstellung und Richtlinien zur Token-Gültigkeitsdauer werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33198 bereitgestellt.
- Aktualisieren von Personen bei Änderung von Azure Active Directory Benutzerkonten.

  Über den neuen Konfigurationsparameter **TargetSystem | AAD | PersonUpdate** kann gesteuert werden, ob bei Änderungen von Benutzerkonten im Azure Active Directory die Eigenschaften der verbundenen Personen im One Identity Manager aktualisiert werden.
- Kundenspezifische Azure Active Directory Schemaerweiterungen werden unterstützt. Der Azure Active Directory Konnektor kann die Azure Active Directory Schemaerweiterungen lesen und schreiben.
- Zur Beschleunigung der Azure Active Directory Synchronisation unterstützt der Azure Active Directory Konnektor das Verfahren der Delta-Synchronisation. Die Delta-Synchronisation ist standardmäßig nicht aktiviert, sondern muss kundenspezifisch eingerichtet werden.
- Für Office 365 Gruppen wird die Eigenschaft **Gruppe in Outlook ausblenden** abgebildet.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34046 bereitgestellt.
- Der Active Directory Konnektor unterstützt Active Directory, welches mit Windows Server 2022 ausgeliefert wird.
- Bei der Active Directory Synchronisation werden restriktivere Werte für die minimale Länge des Kennwortes und die Anzahl der zu speichernden Kennwörter von der globalen Kontenrichtlinie einer Domäne auf die One Identity Manager Kennwortrichtlinie für diese Domäne übernommen.
- Für Active Directory Benutzerkonten wird die Eigenschaft **Zweiter Vorname** abgebildet.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32110 bereitgestellt.
- Der Schutz vor versehentlichem Löschen von Active Directory Container, Benutzerkonten, Kontakten und Computern wird unterstützt.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#32759 und mit der Patch ID VPR#32783 bereitgestellt.

- Für Active Directory Benutzerkonten, Kontakte, Gruppen und Computer wird die Azure AD Connect Anker-ID abgebildet.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#32950 und mit der Patch ID VPR#32952 bereitgestellt.
- Der Password Capture Agent unterstützt Windows Server 2019 und Windows Server 2022.
- Unterstützung von One Identity Active Roles Version 7.4.5.
- Die Active Roles Group Family wird unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34634 bereitgestellt.
- Für Active Roles wird eine neuer Konfigurationsparameter **TargetSystem | ADS | ARS** eingefügt. Active Roles spezifische Bestandteile werden mit einer neuen Präprozessorbedingung **ARS** gekennzeichnet.
- Die Microsoft Exchange Postfachberechtigungen **Senden als** und **Vollzugriff** werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#21073 bereitgestellt. Die Synchronisation ist im Standard nicht aktiviert. Um die Postfachberechtigungen zu synchronisieren, muss das Synchronisationsprojekt angepasst werden.
- Das Ausschließen von Microsoft Exchange Postfachdatenbanken aus der automatischen Postfachverteilung wird unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#26120 bereitgestellt.
- Microsoft Exchange Adressbuchrichtlinien werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#27741 bereitgestellt.
- Für Microsoft Exchange Postfächer wird die Wiederherstellung einzelner Elemente unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31470 bereitgestellt.
- Es wird ein neuer LDAP Konnektor **LDAP Konnektor (Version 2)** zur Verfügung gestellt. Es werden Projektvorlagen für OpenDJ, Active Directory Lightweight Directory Services (AD LDS) und Oracle Directory Server Enterprise Edition (DSEE) sowie eine generische Projektvorlage bereitgestellt.
- Das mehrfache Anbinden von LDAP Systemen mit dem gleichen definierten Namen wird unterstützt.
  - Mit neu erstellten Synchronisationsprojekten wird die Bezeichnung der LDAP Domänen in der Form `<DN Bestandteil 1> (<Server aus Verbindungsparametern>)` gebildet.

    - Für bestehende Synchronisationsprojekte, die mit dem generischen LDAP Konnektor erstellt wurden, wird ein Patch mit der Patch ID VPR#33513 bereitgestellt.
    - Bereits in der Datenbank vorhandene LDAP Domänen werden nicht umbenannt. Passen Sie die Bezeichnung der LDAP Domänen (`Ident_Domain`) gegebenenfalls manuell an.
- Die One Identity Safeguard Versionen 6.7, 6.10 und 6.11 werden unterstützt.
- Zugriffsanforderungen für SSH-Schlüssel für One Identity Safeguard werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32541 bereitgestellt.
- Vault für persönliche Kennwörter für Benutzerkonten in One Identity Safeguard wird unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34392 bereitgestellt.
- Anbindung von PostgreSQL-Datenbanken

  Mit dem generischen Datenbankkonnektor können nun auch PostgreSQL-Datenbanken angebunden werden.
- Der One Identity Manager Konnektor unterstützt die Synchronisation von Datenbanken mit unterschiedlichen Produktversionen oder unterschiedlicher Modulanzahl.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33728 bereitgestellt.
- Generierung von Synchronisationsprojekten für die Synchronisation zweier One Identity Manager-Datenbanken (Systemsynchronisation)

  Das Synchronisationsprojekt für die Synchronisation von zwei One Identity Manager-Datenbanken kann anhand definierter Kriterien automatisch erzeugt werden. Dabei wird ein Abbild ausgewählter Anwendungsdaten einer One Identity Manager-Datenbank erstellt. Revisionsfilterung wird unterstützt. Die Häufigkeit der Synchronisation kann für jede zu synchronisierende Tabelle individuell festgelegt werden.

  Die Systemsynchronisation vereinfacht die Einrichtung und Pflege der Synchronisationskonfiguration. Der One Identity Manager übernimmt das Einrichten aller Komponenten der Synchronisationskonfiguration. Manuelle Anpassungen sind nicht notwendig. Nutzen Sie die Systemsynchronisation beispielsweise um rechenintensive Funktionen wie die Attestierung und den automatischen Entzug von Berechtigungen aus der Zentraldatenbank auszulagern.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33728 bereitgestellt.
- Der Umfang des Synchronisationsprotokolls wurde erweitert. Es werden nun Informationen über die verarbeiteten Objekte, den Synchronisationsfortschritt, die Revisionsfilterung je Synchronisationsschritt ausgegeben. Die Detailtiefe kann an

den Synchronisationsworkflows konfiguriert werden.

- Für die Definition von Quotas können Variablen genutzt werden.
- Der Oracle E-Business Suite Konnektor und der generische Datenbankkonnektor für Oracle Database wurden auf Oracle Data Provider for .NET (ODP.NET) umgestellt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33804 bereitgestellt.

  WICHTIG:

  - Die Verbindungsparameter bestehender Synchronisationsprojekte für Oracle E-Business Suite werden beim Herstellen der Verbindung zum Zielsystem, sofern möglich, angepasst und sollten anschließend geprüft werden.
  - Die Verbindungsparameter bestehender Synchronisationsprojekte für den generischen Datenbankkonnektor für Oracle Database werden bei der Aktualisierung des One Identity Manager, sofern möglich, angepasst und sollten anschließend geprüft werden.
- Abbildung verschiedener Typen von Systemberechtigungen

  Viele Cloud-Anwendungen nutzen mehr als einen Gruppentyp, um Berechtigungen abzubilden. Bei der Anbindung von Cloud-Anwendungen können neben Gruppen nun weitere Typen von Systemberechtigungen, wie Rollen oder Berechtigungssets, abgebildet werden. Abhängig vom Zielsystem werden die Zuweisungen entweder an den Benutzerkonten (benutzerbasierte Zuweisung) oder an den Systemberechtigungen (berechtigungsbasierte Zuweisung) gepflegt. Welche Typen genutzt werden und an welchen Objekttypen die Zuweisungen gepflegt werden, wird beim Einrichten der Synchronisation konfiguriert.

  Die verschiedenen Typen von Systemberechtigungen und deren Zuweisungen können ins Identity Audit und in die Attestierung integriert werden.
- Bei der Definition von Schematypen in einer Schemaerweiterungsdatei für das SAP Konnektorschema können nun auch die Attribute `InsertCommitDefinition`, `WriteCommitDefinition` und `DeleteCommitDefinition` genutzt werden.
- SAP S/4HANA Nutzertypen und Kommunikationsdaten werden unterstützt.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#33301 und VPR#33301_2 bereitgestellt.
- Es wird ein RFC-Funktionsbaustein `/VIAENET/HELPER` mit der Funktionsgruppe `/VIAENET/ZHELPER` bereitgestellt, welcher die Tabelle `PA0002` selektiert.
- Es wird ein RFC-Funktionsbaustein `/VIAENET/READTABLE` bereitgestellt, der sich ähnlich wie der Funktionsbaustein `RFC_READ_TABLE` verhält. Die Funktion kann Daten aus Tabellen und Views in der SAP-Datenbank auslesen, sofern diese nicht als interne Tabellen gekennzeichnet sind.
- Für die Abbildung zusätzlicher HR-Daten an Personen stellt die Synchronisationsvorlage **SAP R/3 HCM employee objects** das Mapping und den Synchronisationsschritt `Employee_PA0000` bereit. Dieses Mapping kann anstelle des Standardmappings `Employee` genutzt werden. Aktivieren Sie dafür den Synchronisationsschritt `Employee_PA0000` und deaktivieren Sie den

Synchronisationsschritt `Employee`.

- Der Domino Konnektor unterstützt Notes Client in der Version 10.0.
- Unterstützung von HCL Domino Server Version 12.0 und HCL Notes Client Version 12.0

  HINWEIS: Wenn die angebundene Domino-Umgebung Domino 12 nutzt und der Domino Konnektor schreibend auf das Zielsystem zugreift, dann muss auf dem Gateway Server die Notes Client Version 12 installiert sein.

  Wenn nur lesend auf das Zielsystem zugegriffen wird, kann auf dem Gateway Server auch eine ältere Notes Client Version genutzt werden.
- Anlegen von SharePoint Online Websitesammlungen und Websites

  Über unternehmensspezifische Anpassungen ist es möglich, Websitesammlungen und Websites im One Identity Manager neu anzulegen und in die SharePoint Online-Umgebung zu publizieren. Zu diesem Zweck werden vordefinierte Skripte und Prozesse bereitgestellt. Diese können als Vorlage genutzt werden, um Websitesammlungen und Websites über den IT Shop bestellbar zu machen.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#31779 bereitgestellt.
- Für die Synchronisation von Unix-basierten Zielsystemen wird die Authentifizierung mit einem privaten SSH-Schlüssel unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33249 bereitgestellt.

Identity Management und Access Governance

- Verbesserte Unterstützung für die Vererbung von zielsystemspezifischen Gruppen und Berechtigungen an Benutzerkonten.

  Um besser zu unterscheiden, welche Arten von Gruppen und Berechtigungen vererbt werden, wurden zusätzliche Optionen für die Vererbung implementiert. Zusätzlich können Sie bereits beim Erstellen der Kontendefinitionen festlegen, welche Gruppen und Berechtigungen vererbt werden sollen. Auf den Überblickformularen der Benutzerkonten wird ein Hinweis angezeigt, wenn Gruppen und Berechtigungen nicht geerbt werden können.
- Für die Vererbung von Gruppen und Berechtigungen anhand von Kategorien können jetzt 64 Kategorien erstellt werden.
- Zuweisungen von Personen an mehrere Geschäftsrollen können verhindert werden. Die Option können Sie für Rollenklassen und Rollentypen aktivieren.
- Neue Standard-Entscheidungsverfahren **KA** und **OT** für Attestierungen und IT Shop-Bestellungen.
- Neues Standard-Entscheidungsverfahren **CS** zur Attestierung von Personen.
- Neue Standardobjekte (Attestierungsrichtlinie, Attestierungsverfahren, Bedingungstypen, Entscheidungsworkflow und Entscheidungsrichtlinie) für die Attestierung der initialen Managerzuordnung. Mit dieser Attestierung können fehlende Managerinformationen an Personen angefordert und zugewiesen werden.

- Neuer Bericht **Übersicht über die Ergebnisse eines Attestierungslaufs**.
- An Attestierungsrichtlinien kann konfiguriert werden, ob der Zertifizierungsstatus von Attestierungsobjekten automatisch geändert werden soll, wenn eine Attestierung genehmigt oder abgelehnt wurde. Die Optionen **Zertifizierungsstatus auf "Zertifiziert" setzen** und **Zertifizierungsstatus auf "Abgelehnt" setzen** können aktiviert werden, wenn am Attestierungsverfahren eine Tabelle ausgewählt ist, die eine Spalte `ApprovalState` hat. Die Funktion kann standardmäßig für die Attestierung von Personen, Geschäftsrollen, Anwendungsrollen und Organisationen genutzt werden.
- Verkürzter Ablauf von Attestierungen, wenn ein Attestierer in einem Attestierungsvorgang mehrfach entscheidungsberechtigt ist. Eine positive Entscheidung dieses Attestierers wird automatisch auf nachfolgende Entscheidungsschritte übernommen. Damit wird der Attestierungsvorgang dem Attestierer nur einmal zur Entscheidung vorgelegt.

  Die Funktion wird über den Konfigurationsparametern **QER | Attestation | ReuseDecision** aktiviert.
- Stichprobenattestierung

  Mit der Stichprobenattestierung können Attestierungsvorgänge auf eine Auswahl an Attestierungsobjekten eingeschränkt werden. Stichproben können manuell oder anhand definierter Kriterien zusammengestellt werden. Es wird eine Standard-Stichprobe **Monatliche organisatorische Änderungen an Personen** bereitgestellt. Diese kann genutzt werden, wenn der Konfigurationsparameter **QER | Selections | PersonOrganizationalChanges** aktiviert ist. Um Zufallsstichproben zu erstellen, kann die SQL-Prozedur `QER_PPickedItemInsertRandom` genutzt werden.
- Bei der Berechnung von Arbeitszeiten, beispielsweise für die Fälligkeit von Attestierungsvorgängen oder die Erinnerung von Entscheidern, werden Wochenenden und Feiertage nun standardmäßig berücksichtigt. Um zu konfigurieren, ob Wochenenden oder Feiertage als Arbeitstage behandelt werden sollen, wurden zusätzliche Konfigurationsparameter eingeführt.
  - QBM | WorkingHours | IgnoreHoliday
  - QBM | WorkingHours | IgnoreWeekend
  - Wenn bei zeitlich begrenzten Bestellungen das Ablaufdatum überschritten ist, können die Bestellungen nun einen Abbestellworkflow durchlaufen, bevor die Zuweisung endgültig entfernt wird.
  - QER | Attestation | UseWorkingHoursDefinition
- Zuweisungen von Unternehmensressourcen an Systemrollen können nun im Web Portal bestellt werden. Dafür wird die Standard-Zuweisungsressource **Zuweisungen an Systemrollen** bereitgestellt.

  Bei der Attestierung von Zuweisungen an Systemrollen können die bestellten Zuweisungen auch automatisch entfernt werden. Dafür wurde der Konfigurationsparameter **QER | Attestation | AutoRemovalScope | ESetHasEntitlement | RemoveRequested** eingeführt.

- Die Definition von SAP Funktionen wurde erweitert, sodass neben Transaktionen auch externe Services, TADIR-Services und RFC-Funktionsbausteine in die Berechtigungsprüfung einbezogen werden können. Transaktionen, externe Services, TADIR-Services und RFC-Funktionsbausteine werden als SAP Applikationen im One Identity Manager abgebildet.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#32963_1 und VPR#32963_2 bereitgestellt.
- Die Definition von produktspezifischen Bestelleigenschaften wurde neu gestaltet. Nun können zahlreiche zusätzliche Informationen für die Bestellparameter definiert werden. Die Bestelleigenschaften sind damit flexibler einsetzbar. Die bisherige Lösung kann weiterhin genutzt werden. Beim Anlegen neuer Bestelleigenschaften legen Sie fest, ob Sie die moderne oder die veraltete Definition nutzen wollen.
- Zugewiesene Bestellungen, deren Ablaufdatum überschritten ist, können nun den an der Entscheidungsrichtlinie hinterlegten Abbestellworkflow durchlaufen, bevor die Zuweisung endgültig entfernt wird. Die Funktion wird über den Konfigurationsparametern **QER | ITShop | ExceededValidUntilUnsubscribe** aktiviert.
- Personen können aufgrund einer abgelehnten Attestierung oder einer Regelverletzung automatisch aus dynamischen Rollen ausgeschlossen werden. Dafür wird eine Ausschlussliste geführt. Zusätzlich können Ausschlüsse auch direkt für einzelne Personen definiert werden.
- Die Reorganisation einer IT Shop-Lösung wird unterstützt. Folgende Aufgaben können für kundendefinierte IT Shop Strukturen ausgeführt werden:
  - Gleichzeitiges Verschieben mehrerer ausgewählter Produkte aus einem Regal in ein anderes Regal.
  - Verschieben eines kompletten Regals in einen anderen Shop.
  - Verschieben eines kompletten Shops in ein anderes Shoppingcenter.
- Einführung einer allgemeinen Stellvertretung für alle Entscheidungsberechtigungen einer Person. Eine Person kann für alle Entscheidungsbefugnisse in einem Bereich einen Stellvertreter benennen. Dieser Stellvertreter wird in einem festgelegten Zeitraum bei allen Entscheidungen, welche die Person zu treffen hat, zusätzlich als Entscheider ermittelt. Stellvertretungen können für die Bereiche Attestierung, Genehmigung von Bestellungen und Ausnahmegenehmigungen von Bestellungen eingerichtet werden.
- Bei der Attestierung von Mitgliedschaften in Anwendungsrollen können auch Mitgliedschaften automatisch entfernt werden, die über eine dynamische Rolle entstanden sind. Dafür wurde der Konfigurationsparameter **QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDynamicRole** eingeführt.
- Google Workspace Admin-Rollen-Zuordnungen können nun im Web Portal bestellt und ins Identity Audit integriert werden.
- Es werden nun auch manuell angelegte Anwendungsrollen für Produkteigner automatisch gelöscht, wenn sie nicht verwendet werden.

HINWEIS: Wenn Sie unterhalb der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** eigene Anwendungsrollen eingerichtet haben, die Sie für kundenspezifische Anwendungsfälle (Tabellen) nutzen, dann prüfen Sie, ob diese automatisch gelöscht werden dürfen. Andernfalls deaktivieren Sie den Zeitplan **Bereinigen der Anwendungsrolle Request & Fulfillment | IT Shop | Produkteigner**.

Siehe auch:

- Verbesserungen auf Seite 16
- Gelöste Probleme auf Seite 32
- Schemaänderungen auf Seite 47
- Patches für Synchronisationsprojekte auf Seite 67

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die im One Identity Manager 8.2 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Der Überblick über die Systemkonfiguration wurde verbessert und um neue Werte erweitert. • Der Bericht kann als CSV-Datei gespeichert werden • Es wird angezeigt, ob die Datenbank verschlüsselt ist. • Die Werte für historische Daten werden besser dargestellt.	31738, 32890, 32992, 34692
Verbesserte Unterstützung des Delta-Verfahrens für die schnellere Aktualisierung von Datenbanken.	32791, 32917
Performanceverbesserung in der Migration.	34109, 34587, 34591
Die Datenbankrolle **basegroup** wird nicht mehr verwendet. Die Datenbankrolle wird bei Neuinstallationen nicht mehr erzeugt. In bestehende Installationen kann die Datenbankrolle weiterhin genutzt werden.	34179
Die Erzeugung von Tabellenindizes wurde verbessert.	33530
Verbesserte Lesbarkeit von generierten Sichtdefinitionen.	31491
Neue Konsistenzprüfung **Mandantory field definition missing** zum Ermitteln potentiell fehlender Pflichtfelddefinitionen.	31297
Die Standardsprache einer Sprachkultur (`QBMCulture.UID_`	31749

Verbesserung	Fehler ID
`DialogCultureDefault`) kann kundenspezifisch geändert werden.	
Für verzögerte Operationen werden jetzt Einträge in der Tabelle `DialogProcess` generiert.	32782
Verbesserte Ermittlung von Prozessinformationen zu einem Auslöser.	34529
Bessere Unterstützung von BULK-Operationen in der Objektschicht.	31066, 31573, 32249
Verbesserte Unterstützung für die Abfrage von historischen Informationen.	30334, 30437, 31449, 31450, 31451, 34723
Erweiterung der EntityLogic-Fluent-Interfaces für bedingte Ausführung.	33796
Optimierte Ermittlung von Anzeigewerten.	33931
Die Hashfunktion SHA-1 wird nicht mehr genutzt.	27488
Verbesserte Berechnung der Kennwortqualität. Die Kennwortqualität für kurze Kennwörter kann jetzt niedriger ausfallen.	33683
Berechtigungen von Anmeldungen für administrative Benutzer mit abgestuften Berechtigungen werden im Configuration Wizard erweitert, sofern dies notwendig ist.	30904
Existierende SQL Server Anmeldungen können im Configuration Wizard verwendet werden.	30791
Verbesserter Aktivierung und Deaktivierung von Authentifizierungsmodulen im Designer.	33929
Die Sektion `<SpecialSheetData>` bei der Konfiguration von Oberflächenformularen wird nicht mehr unterstützt. Die Definition erfolgt jetzt über die Sektion `<Properties>`. HINWEIS: Bestehende Konfigurationen werden während der Aktualisierung der Datenbank angepasst. Prüfen Sie gegebenenfalls die Daten.	31332
Verbesserte Dokumentation der im Standard ausgelieferten Zeitpläne.	32506
Verbesserte Dokumentation für überschreibende Bildungsregeln.	33215
Verbesserte Unterstützung beim Deinstallieren der One Identity Manager-Komponenten. Solange mehrere One Identity Manager-Installationen vorhanden sind, können die Konfigurationsdaten nicht entfernt werden.	31159
Im Verbindungsdialog kann jetzt der Datenbankserver aus der Auswahlliste	32510

Verbesserung	Fehler ID
der Server gelöscht werden.	
Wenn mehrere Datenbanken in einer verwalteten Instanz in Azure SQL-Datenbank betrieben werden, können Sie die Anzahl der Slots über den neuen Konfigurationsparameter **QBM | DBServerAgent | CountSlotAgents** fest vorgeben.	34047
Verbesserte Unterstützung der nachträglichen Installation von Modulen.	33942
Verbesserte Dokumentation der Reinitialisierung des DBQueue Prozessor nach Erweiterung des Serverhardware.	34208
Der `StdIoProcessor.exe` prüft, ob sein übergeordneter Prozess (`VINetworkService.exe`) noch erreichbar ist und funktioniert.	31081
Verbesserte Protokollierung der Prozessverarbeitung in der Protokolldatei des One Identity Manager Service.	31536, 32792, 33721, 34330, 34559
Verbesserte Ausgabe der Tabellennamen in Fehlernummer 810005.	31686
Neue Maschinenrolle **Server\Job Server\Konfigurationswerkeug** für die Installation von Job Service Configuration.	32776
Der Server Installer merkt sich das Verzeichnis mit den Installationsdateien.	33686
Verbesserte Installationsinformationen für den One Identity Manager Service im Server Installer und im Configuration Wizard.	34457
Beim Beenden des One Identity Manager Service ist nun eine Zeitverzögerung wirksam, damit der Dienst sich mit der Datenbank synchronisieren kann.	34459
Kundenspezifische Übersetzungen für Texte aus Ressourcendateien werden unterstützt.	23677
Der Where-Klausel-Assistent zur Eingabe von Datenbankabfragen unterstützt Datumsvergleiche.	17996
Verbesserte Rückmeldung für den Systemstatus in der Statuszeile in den One Identity Manager-Werkzeugen.	29567
In der Statuszeile wird angezeigt, ob der angemeldete Benutzer ein administrativer Benutzer ist.	33491
Aktualisierung der Steuerelemente in den One Identity Manager- Werkzeugen.	31577
Verbesserte Darstellung von mehrzeiligen Werten in MVP-Spalten.	31312

Verbesserung	Fehler ID
Verbesserter Darstellung von Spalten, die ein URL repräsentieren.	33545
Wenn ein Text zu lang zur Übersetzung ist, wird jetzt ein entsprechender Hinweis am Eingabefeld angezeigt.	33667
Um Filter allen Benutzern zur Verfügung zu stellen, können Sie die Filter veröffentlichen, beispielsweise im Manager oder im Designer.	31025, 33247
Verbesserte Darstellung des Primärschlüssels im Eigenschaftendialog eines Objektes. Der Primärschlüssel kann in verschiedenen Formaten kopiert werden.	32549
Verbesserter SQL-Export im Eigenschaftendialog eines Objektes.	33679
Verbesserte Unterstützung für die Skriptbearbeitung. • Die Funktionen im erweiterten Bearbeitungsfenster für Skripte wurden überarbeitet und erweitert. • Es werden zusätzliche Code-Ausschnitte bereitgestellt. • Die Sortierung für Code-Ausschnitte wurde verbessert.	32026, 32937, 33161, 33162, 33240
Für Berichtsparameter können Anzeigewerte an Berichte übergeben werden.	34272
Die maximale Anzahl von Ergebniszeilen von Berichtsabfragen kann jetzt kundenspezifisch angepasst werden.	34293
Auf Zuweisungsformularen im Manager werden Tooltipps angezeigt.	31634
Auf den Zuweisungsformularen werden die ausstehenden Objekte jetzt durchgestrichen angezeigt.	34508
Im Object Browser werden Breakpoints beim Schließen des Debug-Dialoges automatisch in die Konfiguration gespeichert und beim erneuten Öffnen des Debug-Dialoges von dort geladen.	30816
Verbesserte Nachfrage beim Speichern von Änderungen im Object Browser.	31291
Im Object Browser werden bei der Ausführung von SQL Abfragen die Gesamtanzahl der Zeiten und die Ausführungsdauer der Abfrage ausgegeben.	31813
Erweiterungen und Verbesserungen im Job Queue Info. • Parameter, die einen Objektschlüssel enthalten, werden als Link dargestellt. Über den Link werden die Objekteigenschaften angezeigt. Es kann der Object Browser gestartet werden. Für Objektschlüssel, die auf ein Synchronisationsprojekt verweisen, kann der Synchronization Editor gestartet werden. • Es kann eine neue Startzeit für einen Prozessschritt festgelegt	30102, 31983, 32851, 33516, 33642

Verbesserung	Fehler ID
werden. • Die Anzahl der Wiederholversuche für einen Prozessschritt kann geändert werden. • Es können mehrere Jobserver gleichzeitig ausgewählt werden, um die Anmeldeinformationen für die Statusermittlung zu bearbeiten.	
Im Software Loader wird der Basisverzeichnis jetzt pro Datenbank gespeichert.	29507
Prüfung im Database Transporter, ob der angemeldete Benutzer ausreichende Berechtigungen für den Import hat.	34704
Verbessertes Verhalten des Webservice-Integrationsassistenten.	31425
Verbesserte Unterstützung für Maildefinitionen im Designer.	31820, 33419
Im Designer werden geänderte Konfigurationsparameter im Konfigurationsparametereditor speziell gekennzeichnet.	32566
Verbesserte Unterstützung zum Bearbeiten von Tabellenbeziehungen. Dynamische Tabellenrelationen werden jetzt im Schemaeditor angezeigt.	31849, 32582, 32429
Sichtdefinitionen können im Schemaeditor geprüft werden.	33170
Im Skripteditor kann die Schriftgröße mittels **Strg + Mausrad** verändert werden.	32026
Der Prozesseditor weist bei der Gültigkeitsprüfung von Prozessen auf mögliche Fehlkonfigurationen hin.	32035, 34223
Verbesserte Unterstützung der Spaltenkonfiguration im Schema Extension.	32436
Verbessertes Verhalten der Kommandozeilenwerkzeuge. • Version, Fehlermeldungen und Hilfetexte werden ausgegeben. • Im Parameter `/conn` der Kommandozeilenwerkzeuge kann der Name der Verbindung laut Registrierungsdatenbank `HKEY_CURRENT_USER\Software\One Identity\One Identity Manager\Global\Connections` eingetragen werden.	30328, 31082, 34077, 34209, 33010
Im Kommandozeilenprogramm `DBTransporterCMD.exe` wird besser erkannt, wann kompiliert werden muss.	32062
Verbesserte Unterstützung beim Importieren von Dateien mit dem Kommandozeilenprogramm `SoftwareLoaderCMD.exe`.	33943
Dokumentation des Kommandozeilenprogramms `create-web-dir.exe`.	33618
Beim Schließen des Launchpad über die Schaltfläche **Schließen**, wird jetzt	31984

Verbesserung	Fehler ID
ein Hinweis angezeigt, dass das Launchpad in den Infobereich der Windows Taskleiste minimiert wird.	
Das Launchpad zeigt die Farbe der Staging-Ebene in der Statuszeile an.	32593
Die Powershell-Bibliothek für One Identity Manager wurde erweitert.	33127

Tabelle 2: Allgemein Webanwendungen

Verbesserung	Fehler ID
Verbesserte Sicherheit im Anwendungsserver.	32466
Erweiterungen und Verbesserungen der Anwendungsserver REST API.	32576, 33963, 33728, 33126, 32930, 33923, 34016
Verbessertes Session-Handling im Anwendungsserver, wenn über Token authentifiziert wird.	33406
Die Gültigkeit des Session-Zertifikates wird geprüft.	32141
Im Anwendungsserver ist es jetzt möglich, mit Anfragen, die durch Zugriffstoken authentifiziert wurden, auf die API zuzugreifen.	245784
Der Web Designer-Konfigurationsschlüssel **VI_ITShop_Compliance_DoNotCheckIndirect** wurde entfernt.	33042
Aus Sicherheitsgründen kodiert die Web Designer-Komponente **VI_Common_UserMessageAdd HTML** den eingegebenen Text nun standardmäßig. Dieses Verhalten kann durch die virtuelle Funktion `DoNotHtmlEncode()` beim Aufruf der Komponente abgeschaltet werden.	202604
Aus Sicherheitsgründen kann die Web Designer-Komponente **VI_Common_ExternalFormHost** nun nicht mehr dazu verwendet werden, beliebige URLs anzuzeigen. Falls Sie diese Funktionalität benötigen, müssen Sie existerenden Code umbauen und stattdessen die Formularkomponente **QBM_Common_ExternalFormHost** verwenden. Diese bietet den Vorteil, dass URLs nicht in Form von URL-Parametern übergeben werden.	203559
Der Parameter **withPermissions** der Web Designer-Funktion `dbcount()` wird nun als obsolet gekennzeichnet.	34222
Die Berechtigungen zum Debuggen von Webanwendungen wurden erweitert.	34308
Webauthn-Sicherheitsschlüssel: Die RSTS-Version wurde auf Version	206688

Verbesserung	Fehler ID
2019.11.22.0 aktualisiert. Sie können nun verhindern, dass der X-Frame-Options HTTP-Response-Header überhaupt ausgegeben wird, indem Sie die RSTS-Konfigurationseigenschaft **DisableAddingXFrameOptionsHeader** auf **true** setzen.	
Identitäten mit der Anwendungsrolle **Basisrollen | Betriebsunterstützung** können nun nicht mehr die DBQueue und Jobqueue starten und stoppen. Sollen Identitäten diese Aufgaben durchführen, muss ihnen die Anwendungsrolle **Basisrollen | Betriebsunterstützung | Systemadministratoren** zugewiesen werden.	34368
Die Performance des Grid-Steuerelements wurde verbessert. Es werden weniger Datenbankabfragen erzeugt.	206856
Wenn aus einem Einkaufswagen eine Bestellposition entfernt wird, welche abhängige Produkte hat, werden auch die abhängigen Bestellpositionen entfernt.	32758
Wenn ein Einkaufswagen gelöscht wird, werden dessen Bestellpositionen ebenfalls gelöscht.	33342
Verbesserte Darstellung der Ergebnisse einer Peer-Gruppen-Analyse.	34190
Manager sehen nun im Web Designer Web Portal und im Web Portal alle Delegierungen ihrer unterstellten Identitäten.	33774
Es kann nun eine Standardgröße für Bilder festgelegt werden. Beim Hochladen von Bildern ins Web Portal werden diese dann entsprechend skaliert.	32916
Bereits abgesendete Einkaufswagen werden jetzt entsprechend gekennzeichnet und es ist nicht mehr möglich, weitere Produkte zu solchen Einkaufswagen hinzuzufügen.	33143
Im Web Portal wird nun in den Stammdaten einer Bestellung statt des Bearbeitungsstatus der Status der Bestellung angezeigt.	34181
Für das Web Portal wurden verbesserte Warnungen für die Protokolldatei und für die Web Portal Monitor-Seite eingeführt, die auf Komponenten hinweisen, die auffällig viele Objekte laden.	206672
Die Kontrollkästchen vor Datumsfeldern im Web Portal wurden entfernt. Möchte man nun keine zeitliche Einschränkung vornehmen, reicht es, die Felder nicht auszufüllen.	206732
Endet eine Single-Sign-On-Sitzung im Web Designer Web Portal, wird nun eine Schaltfläche angezeigt, mit der man sich erneut über Single-Sign-On anmelden kann.	206886
Im Web Portal ist die Menge auswählbarer Referenzbenutzer in der	246899

Verbesserung	Fehler ID
Standardkonfiguration eingeschränkt.	
Der Dialog zum Löschen von sekundären Mitgliedschaften einer Rolle im Web Portal wurde erweitert. Er bietet nun die Möglichkeit, jeweils die direkten, bestellten und dynamischen Mitgliedschaften optional zu löschen.	250631
Mitgliedschaften in Systemberechtigungen sind nun im Web Portal filterbar und paginierbar.	275192
Die Beschriftung im Filterdialog **Filterung auf <Spaltenname>** wurde geändert auf **Filterung auf die Spalte '<Spaltenname>'**.	274174
Die Eingabe eines fehlerhaften Datums im Web Portal erzeugt nun eine Fehlermeldung.	33056
Folgende Spalten an in der Tabelle `QBMWebApplication` wurden so beschrieben, dass erkenntlich wird, dass sie nur für das Web Designer Web Portal relevant sind: • UID_DialogAEDSWebProject • UID_DialogAuthentifier • UID_DialogAuthSecondary	34334
Das Design und die Benutzerführung des Web Portal für Betriebsunterstützung wurde verbessert.	278209
Aus Performance-Gründen wurde das API Server-Ergebnisformat geändert, sodass der Wert von **DisplayValue** nur noch mitgeschickt wird, sofern er sich vom Wert von **Value** unterscheidet.	206530
Für den API Server wurde die API-Methode `imx/ping` eingeführt. Diese API-Methode kann als "Health Check" des API Servers verwendet werden. Sie ist ohne Authentifizierung aufrufbar.	206652
Es ist nun möglich das Logging des API Servers über eine zentrale Konfigurationsdatei zu konfigurieren.	206728
Der API Server gibt nun nicht gesetzte Datumswerte in der JSON-Serialisierung als **NULL** zurück.	239140
Für den API Server wurde die Komponente Microsoft Extensibility Framework entfernt. HINWEIS: • Die Markierung von Klassen mit den Attributen `[Export]` oder `[Import]` wird nicht mehr unterstützt. • Alle öffentlichen Klassen, die ein bestimmtes Interface implementieren, werden automatisch als Plugin gefunden. • Plugin-Klassen dürfen nicht mehr als "internal" markiert sein.	240595

Verbesserung	Fehler ID
Plugin-Klassen müssen einen öffentlichen und parameterlosen Konstruktor definieren.	
Der API Server unterstützt nun HTTP-Komprimierung.	265172
Für HTML5-Anwendungen wurde eine Content-Security-Policy eingeführt.	203857
Die Quelltextstruktur für HTML5-Anwendungen wurde auf einen Angular Workspace umgestellt, um eine einheitliche Ordnerstruktur ohne symbolische Verknüpfungen zu ermöglichen.	226217
Der API Server stellt die Dokumentation der HTML5-Webanwendungen zur Verfügung.	268196
Abgebrochene Anfragen erscheinen nicht mehr im Log von HTML5-Webanwendungen.	271770
Aus Performance-Gründen kann nun bei der Konfiguration Entity-basierter API-Methoden die Verarbeitung von Entities im Bulk-Verfahren konfiguriert werden.	228139
Das Entity-Schema muss nun zur Laufzeit vom API Server abgefragt werden.	251938
Folgende Änderungen wurden am API-Modell für hierarchische Entity-Strukturen vorgenommen: • Das Flag **DisableHierarchicalData** in der API-Definition wurde abgeschafft. • Der URL-Parameter **noRecursive** wurde abgeschafft. Über den URL-Parameter **ParentKey** kann gesteuert werden, ob Ergebnisse aus der obersten, einer bestimmten oder aus allen Hierarchieebenen zurückgegeben werden sollen.	273103

Bei der Definition einer API-Methode werden nicht mehr alle Spalten standardmäßig schreibbar gemacht. Beim Entwickeln von API-Methoden müssen die Spalten einzeln deklariert oder explizit alle schreibbar gemacht werden.
Beispiel:
`Method.Define("some_url")`
`.From("Person")`
`.EnableUpdate()`
`.WithWritableColumns("FirstName", "LastName")`
	274045

Der Internet Explorer wird nicht mehr unterstützt.	273336
Aktualisierung der Secure Password Extension auf die Version 5.9.5.	34834

Tabelle 3: Zielsystemanbindung

Verbesserung	Fehler ID
Es werden Customizer-Methoden bereitgestellt, um ausstehende Objekte automatisiert zu behandeln. Diese Methoden können in Skripten oder Prozessen aufgerufen werden.	29566
Verbesserte Protokollierung von Synchronisationsfehlern mittels NLog.	30992
Verbesserte Dokumentation von Quotas in Synchronisationsschritten.	31927
Der Synchronisationspuffer kann für Schemaeigenschaften im One Identity Manager Schema, die Mitglieder von M:N Schematypen oder Schlüsselauflösungen abbilden, deaktiviert werden. WICHTIG: Wenn der Synchronisationspuffer deaktiviert ist, werden bei der Synchronisation in das Zielsystem oder bei der Provisionierung die Referenzen, die im One Identity Manager fehlen, im Zielsystem gelöscht. Prüfen Sie daher sorgfältig, ob der Synchronisationspuffer deaktiviert werden kann.	31947
Neue Konsistenzprüfung **Outstanding objects with not outstanding assignments** zum Ermitteln ausstehender Objekte mit Zuweisungen, die nicht ausstehend sind.	32058
Der Synchronization Editor kann im Offline-Modus ausgeführt werden, wenn kein Zugriff auf das verbundene System notwendig ist.	32181
Der One Identity Manager Konnektor erkennt, ob der Customizer Standardwerte für Pflichtfelder setzt.	32346
Beim automatischen Erstellen oder Aktualisieren von Synchronisationsprojekten per Kommandozeilenbefehl oder Windows PowerShell CmdLet kann für die Verbindung zum Zielsystem nun auch eine Remoteverbindung genutzt werden.	32411
In der Protokollansicht des Synchronization Editor wird farblich gekennzeichnet, ob eine Synchronisation erfolgreich oder mit Fehlern beendet wurde.	32517
Beim Einrichten eines neuen Synchronisationsschritts wird für Objekte im One Identity Manager für die Verarbeitungsmethode `Delete` standardmäßig eine Quota von **10 %** festgelegt. Diese Quota sollte projektspezifisch angepasst werden.	32740
Auf der Startseite des Synchronization Editor wird angezeigt, ob für bestehende Synchronisationsprojekte Patches bereitstehen.	32795
Um eine Startfolge erneut ausführen zu können, wenn sie abgebrochen wurde, kann die Instanz der Startfolge direkt im Synchronization Editor gelöscht werden.	33050
In der Schemaansicht des Mappingeditor wird nun angezeigt, welche	33064

Verbesserung	Fehler ID
Schemaeigenschaft den Revisionszähler enthält.	
Im Synchronization Editor können nun Kopien von Synchronisationsprojekten angelegt werden.	33280
Verbesserung der Provisionierung von Mitgliedschaften, wenn die Mitglieder eines Objekts im One Identity Manager auf verschiedene Mitgliederlisten eines Objekts im Zielsystem gemappt sind.	33449
Schemaeigenschaften mit dem Eigenschaftstyp **Eigenschaftsverbindung** (`PropertyJoin`) sind nun schreibbar.	33417
In Synchronisationsprojekten mit dem generischen Datenbankkonnektor, dem Windows PowerShell Konnektor und dem CSV Konnektor kann für jedes verbundene System ein Subtyp erfasst werden. Der One Identity Manager benötigt diese Information für die Provisionierung von Mitgliedschaften, wenn die Objekte aus mehreren gleichartigen generischen Zielsystemen in den gleichen One Identity Manager Tabellen abgebildet werden.	33426
Der Synchronization Editor verhindert, dass Synchronisationsprojekte gleichzeitig durch mehrere Benutzer bearbeitet und gespeichert werden.	33753
Verbesserter Unterstützung der Revisionsfilterung.	34101, 34102
An Startfolgen kann das Verhalten konfiguriert werden für den Fall, dass eine Startfolge mehrfach gestartet wird, obwohl mehrfache Starts nicht zugelassen sind. Die neue Instanz der Startfolge kann mit Fehler abgebrochen (Standardverhalten) oder stillschweigend beendet werden.	34114
Bessere Fehlermeldung zum Fehler: `Automatic resolution of the failed workflow's dependencies.`	34140
Mit dem Synchronization Editor Command Line Interface kann das One Identity Manager Schema in Synchronisationsprojekten aktualisiert werden.	34117
Die Bedingung für die Anwendung einer Property-Mapping-Regel kann nun auch als Skript formuliert werden.	34285
Im Systemverbindungsassistenten können fehlerhafte Verbindungsparameter bereinigt werden.	34367
Ein neuer Konsistenztest prüft, ob die Systemverbindung schreibbar ist, wenn an einer Property-Mapping-Regel **Unzulässige Änderungen korrigieren** aktiviert ist.	34576
Verbesserte Darstellung der Meldungen im Synchronisationsprotokoll.	34691
Verbesserte Anzeige der Herkunft von Azure Active Directory Abonnements	32744

Verbesserung	Fehler ID
und Dienstplänen für Personen.	
Verbesserte Dokumentation der Besonderheiten, Empfehlungen und notwendigen Anpassungen beim Betrieb einer Azure Active Directory Verbund-Umgebung.	33378
Verbesserte Unterstützung der Verknüpfung von Azure Active Directory Benutzerkonten und Active Directory Benutzerkonten in Azure Active Directory Verbund-Umgebungen.	34051
Verbesserte Behandlung der Eigentümer von Azure Active Directory Gruppen beim Löschen von Gruppen.	33653
LDAP Container können umbenannt werden.	34134
Für LDAP Attribute werden jetzt im Synchronization Editor die Syntax-Regeln zusätzlich zu den Beschreibungen angezeigt.	33434
Verbesserter Umgang mit Multi-Forest-Strukturen bei der DNS Auflösung des Globalen Kataloges. Der Algorithmus zur Suche im Globalen Katalog beachtet jetzt die Active Directory Forest-Root-Domäne bei der Suche.	31179
Verbesserte Anzeige der Active Directory Objekte im Manager und in Berichten. Es wird jetzt der vollständiger Domänenname (`ADSDomain.ADSDomainName`) für die Darstellung verwendet.	32242
Die Schemaeigenschaften `member` von Active Directory Gruppen ist im Zielsystembrowser schreibgeschützt, um Schreibvorgänge zu verhindern, die zu fehlerhaften Ergebnissen führen würden, wenn eine Gruppe mehr als 1500 Mitglieder hat. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34324 bereitgestellt.	34324
Verbesserte Unterstützung von dynamischen Gruppen in Active Directory.	34769, 34632
Verbesserte Protokollierung im Active Roles Konnektor.	33801
Verbesserte Behandlung von dynamischen Gruppen in Active Roles.	34287, 34323, 34627
Die Microsoft Exchange Richtlinie für mobile E-Mail Abfragen wurde umbenannt in **Postfachrichtlinie für mobile Geräte**.	27741
Die Beschriftung der Spalte `PAGAccessOrder.ValidDurationMinutes` wurde geändert in **Gültigkeitsdauer [Min]**.	34678
In die Prozesse `ADS_ADSDomain_Publish ADSGroups to ITShop_PostSync` und `AAD_AADOrganization_Publish AAD objects to ITShop_PostSync` wurde ein Warte-Schritt aufgenommen, der prüft, ob der jeweilige Prozess zur	34651, 34658

Verbesserung	Fehler ID
automatischen Zuordnung von Personen zu Benutzerkonten (`ADS_ADSDomain_SearchandCreate_Person_PostSync` und `AAD_Organization_SearchAndCreate_Person_PostSync`) beendet ist.	
Im Systemverbindungsassistenten für Cloud-Anwendungen kann eine Referenzzeitzone für die Behandlung von Datumswerten ohne UTC Offset hinterlegt werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33978 bereitgestellt.	33978
Der generische Datenbankkonnektor für den generischen ADO.NET Provider unterstützt jetzt das Zurücklesen automatisch gebildeter Wert.	34104
Verbesserter Protokollierung im generischen Datenbankkonnektors.	34823
Verbesserte Unterstützung von dynamischen Gruppen in kundendefinierten Zielsystemen.	34632
Es werden zusätzliche Berichte über Benutzerkonten und Gruppen in allen Zielsystem bereitgestellt.	33456, 33599
Verschiedene Berichte zeigen jetzt auch die Herkunft einer Mitgliedschaft oder einer Berechtigung an.	27414
Es werden weitere Einstellungen zur Zugriffssteuerung für Google Workspace Gruppen abgebildet. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32610 bereitgestellt.	32610
Der Schematyp `HROrgUnitManager` wurde erweitert, sodass nun auch der Gültigkeitszeitraum von Managerzuordnungen abgebildet werden kann.	33209
Die Standardfirma von SAP Mandanten kann nun durch die Synchronisation eingelesen werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33819 bereitgestellt.	33819
Für Zielsysteme im Unified Namespace wird im Manager ein Überblicksformular angezeigt.	33412
Das Überblicksformular für E-Business Suite Systeme (`VI_EBS_EBSSystem_Overview`) zeigt einen Hinweis, wenn kein Synchronisationsprojekt eingerichtet wurde.	34380
Der Windows PowerShell Konnektor und der One Identity Safeguard Konnektor behandeln Kennwörter nun als geheime Werte. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34403 bereitgestellt.	34403

Verbesserung	Fehler ID
Die Eigenschaft `edsaIsDynamicGoup` von Active Directory Gruppen wird im One Identity Manager abgebildet. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34168 bereitgestellt.	34168
An Google Workspace Benutzerkonten werden weitere Schemaeigenschaften abgebildet. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33093 bereitgestellt.	33093
Der SCIM Konnektor lässt nun maximal 10 parallele Zugriffe zum Lesen von Einzelobjekten während der Synchronisation zu. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32564 bereitgestellt.	32564
Für die Synchronisation von Cloud-Anwendungen über das Universal Cloud Interface kann nun konfiguriert werden, ob die Verbindung zum Zielsystem bestehen bleiben soll. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33884 bereitgestellt.	33884

Tabelle 4: Identity Management und Access Governance

Verbesserung	Fehler ID
Zusätzliche zulässige Werte für `Person.ImportSource`.	24169
Für automatische Entscheidungen von Bestellungen und Attestierungsvorgängen gilt nun: Wenn durch eine Neuberechnung der verantwortlichen Entscheider zusätzliche Entscheider ermittelt werden, dann wird der Zeitpunkt für die automatische Entscheidung dadurch nicht verlängert. Die zusätzlichen Entscheider müssen innerhalb des Zeitraums entscheiden, der für die bisherigen Entscheider gültig ist.	33182
Benutzerkonten, denen absichtlich keine Person zugeordnet ist, können entsprechend gekennzeichnet werden. Wenn die Attestierung von Benutzerkonten, die nicht mit einer Person verbunden sind, genehmigt wird, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Person verbunden sind, nach verschiedenen Kriterien gefiltert werden.	33384, 34387
An Attestierungsverfahren können Textvorlagen hinterlegt werden, welche den zu attestierenden Sachverhalt beschreiben. Dieser Text wird den Attestierern im Web Portal angezeigt.	33494
Performanceverbesserungen beim Erstellen von Attestierungsvorgängen und Attestierungsläufen.	33742, 34017,

Verbesserung	Fehler ID
	34039, 34202, 34217, 34243, 34344, 34431
An Attestierungsrichtlinien kann eine Anwendungsrolle als Eigentümer zugeordnet werden, sodass mehrere Personen Eigentümer einer Attestierungsrichtlinie sein können.	33783
An Attestierungsrichtlinien kann die Sprache definiert werden, in der die zu attestierenden Informationen angezeigt werden sollen.	34148
Es werden zusätzliche Berichte über Attestierungsläufe bereitgestellt, welche die komplette Attestierungshistorie enthalten.	34203
An Standard-Attestierungsverfahren können nun auch kundendefinierte Berichte zugeordnet werden.	34569
Mailvorlagen, die für die Benachrichtigung von Regel- und Richtlinienverantwortlichen sowie Ausnahmegenehmigern genutzt werden, werden nun direkt den Complianceregeln und Unternehmensrichtlinien zugeordnet. Folgende Konfigurationsparameter wurden gelöscht: • QER | Policy | EmailNotification | NewExceptionApproval • QER | Policy | EmailNotification | NotPermittedViolation • QER | ComplianceCheck | EmailNotification | NewExceptionApproval • QER | ComplianceCheck | EmailNotification | NotPermittedViolation Bei der Aktualisierung der One Identity Manager-Datenbank werden die Werte der Konfigurationsparameter in die neuen Spalten `ComplianceRule.UID_DialogRichMailNewViolation` und `QERPolicy.UID_DialogRichMailNewViolation` übernommen.	31781
Entscheidungsschritte können nun auch dann eskaliert werden, wenn kein Entscheider oder Attestierer ermittelt werden kann und kein Fallback-Entscheider zugeordnet ist. Die Bestellung beziehungsweise der Attestierungsvorgang wird in diesem Fall nicht mehr abgebrochen oder an die zentrale Entscheidergruppe übergeben, sondern eskaliert.	27902
Das Entscheidungsverfahren **CM** kann nun auch für die Attestierung der Zuweisungen von Systemrollen und von Kontendefinitionen an Personen genutzt werden.	34290
Beim Versenden von E-Mail-Benachrichtigungen im IT Shop und bei Attestierungen wird nun standardmäßig die Absenderadresse angegeben,	32072

Verbesserung	Fehler ID
die an den Konfigurationsparametern **QER | Attestation | DefaultSenderAddress** und **QER | ITShop | DefaultSenderAddress** eingetragen ist. Die Standard-E-Mail-Adresse der Person wird nicht mehr als Absenderadresse für automatische Benachrichtigungen verwendet.	
Die Berechtigungen für die Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** wurden erweitert.	32185
Auf den Überblicksformularen von Abteilungen, Standorten, Kostenstellen, Geschäftsrollen, Anwendungsrollen und IT Shop Strukturen werden vorhandene Delegierungen für den Manager und 2. Verantwortlichen angezeigt.	32682
Performanceverbesserungen beim Speichern von Bestellungen.	33898
Neue Konsistenzprüfung **Direct memberships in BaseTree that are not allowed** zur Ermittlung von direkten Zuweisungen an Rollen und Organisationen, für die eine direkte Zuweisung nicht erlaubt ist.	34060
Die Neuberechnung einer dynamischen Rolle kann zeitweilig deaktiviert werden (`DynamicGroup.IsRecalculationDeactivated`).	34076
Über die Variable `@UID_Org` können Sie auf die Rolle oder die Organisation zugreifen, auf welche die dynamische Rolle verweist.	33757, 31554
Verbesserte Berechnung von dynamischen Rollen.	29973
Der Nutzungstyp von Standardbegründungen kann nun durch Anwender bearbeitet werden	34218
Die Konfigurationsparameter für die automatische Übernahme von Gruppen in den IT Shop wurden umstrukturiert. Der bisherige Konfigurationsparameter **QER | ITShop | GroupAutoPublish** und der Präprozessorausdruck `GroupAutoPublish` galt für Active Directory und SharePoint Gruppen. Das wurde aufgeteilt. Der Präprozessorausdruck `GroupAutoPublish` wird weiterhin mit dem neuen Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup** genutzt. Für den neuen Konfigurationsparameter **QER | ITShop | AutoPublish | SPSGroup** wurde der Präprozessorausdruck `AutoPublish_SPSGroup` eingeführt. HINWEIS: Wenn Sie kundenspezifische Anpassungen für SharePoint Gruppen implementiert haben, welche den Präprozessorausdruck `GroupAutoPublish` nutzen, dann ändern Sie dafür den Präprozessorausdruck auf `AutoPublish_SPSGroup`.	34310
Zusatzeigenschaften können jetzt auch an LDAP Container zugewiesen werden.	34401
Verbesserte Vorbereitung von Daten für eine schnellere	31167

Verbesserung	Fehler ID
tabellenübergreifende Suche. Es kann jetzt zusätzlich ein Pfad zum Person-Objekt angegeben werden, um die Person innerhalb der tabellenübergreifenden Suche für Benutzerkonten oder E-Mail-Adressen zu ermitteln.	
Beim automatischen Erzeugen von Anwendungsrollen für Produkteigner wird jetzt der Anzeigenamen der Person zur Bildung der Bezeichnung der Anwendungsrollen verwendet.	34602
Beim Absenden von Bestellungen wird das Gültig-bis-Datum nicht mehr gegen die aktuelle Uhrzeit geprüft. So werden beispielsweise Fehler vermieden, wenn zwischen Anlegen und Absenden eines Einkaufswagens längere Zeit verstrichen ist.	34621

Siehe auch:

- Schemaänderungen auf Seite 47
- Patches für Synchronisationsprojekte auf Seite 67

Gelöste Probleme

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

Tabelle 5: Allgemein

Gelöstes Problem	Fehler ID
Parameterwerte werden nicht vollständig aus der Prozess-Simulation in die Zwischenablage übernommen.	32724
Blockaden beim Ausführen von `QBM_PProcessGroupDelete` aus dem Übernahmeprozess für die History Database.	34796
Die statischen Methoden der `DateRange`-Klasse nehmen die Zeitzonenkonvertierung noch nicht richtig vor.	33009
Es können Objektdefinitionen (`DialogObject`) ohne Verweis aus eine Tabelle erstellt werden.	33155
Fehler im Schemaeditor beim Bearbeiten von Tabellen und Spalten.	33429
Datumsangaben mit der Uhrzeit 0:00 werden nicht korrekt in UTC-Format umgerechnet.	33472
Es ist nicht möglich, Datenbanken mit einem Namen mit mehr als 40 Zeichen zu erstellen.	33549, 33906
Hoher Speicherverbrauch beim Kompilieren mit dem Configuration Wizard	33563

Gelöstes Problem	Fehler ID
oder dem Database Compiler.	
Die automatische Softwareaktualisierung berücksichtigt nicht, dass nur Dateiaktionen ausgeführt werden sollen.	34454
Beim Weiterschalten von Prozessschritten mit dem Status **Frozen** in Job Queue Info verliert der nachfolgende Prozessschritt seine Wiederholversuche.	34496
Eine Änderung an der Option **UseSSL** in der Konfiguration des One Identity Manager Service verlangt einen Neustart des Dienstes, obwohl die laut Anzeige im Job Service Configuration nicht notwendig sein sollte.	34525
Fehler in der Prozedur `QBM_PDBQueueRunner` beim Entfernen von Modulen.	34555
Fehler bei der Anmeldung an der Manager Webanwendung mit japanischen Sprache.	34558
Beim Testen, ob ein Bericht Daten enthält, tritt unter Umständen ein Fehler auf. Fehlermeldung: `Could not find stored procedure 'Report_LimitData'.`	34596
Die Eingabe einer Zeichenkette für die Prozessinformation eines Ereignisses führt zu einem Fehler bei der Kompilierung. Fehlermeldung: `'<Text>' is not declared. It may be inaccessible due to its protection level.`	34716
Daten, die über den Anwendungsserver bereitgestellt werden, enthalten für Fremdschlüssel kein **NULL** sondern eine leere Zeichenkette.	34720
Fehler im Schema Extension beim Erstellen einer kundendefinierten Tabelle mit einem Fremdschlüssel zu einer `Basetree*`-Sicht.	34749
Fehler in der Konsistenzprüfung **DialogDeferredOperation with overdue actions, activated but without existing job**.	34765
Der Trigger `QER_TIPersonInBaseTree` zur Prüfung von `BaseTreeExcludesBaseTree`-Verstößen beachtet die Spalte `XOrigin` nicht.	34519
Beim Erzeugen einer Vorschau für einfache Listenberichte kann es unter Umständen zu Fehlern kommen.	34752
In Berichten wird das Mindestdatum (30.12.1899) nicht mehr korrekt ausgeblendet.	34550
Ein Systembenutzer, der nur Leseberechtigungen besitzt, erhält durch Programmfunktionen unter Umständen zusätzliche Änderungsberechtigungen.	34812
Beim Ändern des Kennwortes für ein Benutzerkonto wirft der Customizer einen Fehler, wenn die Änderung nicht gespeichert wird, sondern	33594

Gelöstes Problem	Fehler ID
verworfen wird.	
Fehler im Reparaturskript der Konsistenzprüfung **Missing tables in dialogtable (base)**.	34846
Beim Speichern von Bildungsregeln im System Debugger verschwindet der Code, wenn im Code ein `<summary>`-Block enthalten ist.	34404
Bildungsregeln werden beim Speichern im System Debugger nicht zum Änderungskennzeichen gebucht.	34412
Für Übersetzungen werden nicht alle Sprachabhängigkeiten beachtet.	34410
`DialogWatchOperation.OperationUser` wird unter Umständen nicht befüllt.	34429
Fehler beim Öffnen des TimeTrace im Manager.	34449

Tabelle 6: Allgemein Webanwendungen

Gelöstes Problem	Fehler ID
Die Schaltfläche **Neue untergeordnete Gruppe** enthält die Sichtbarkeitsbedingung **CanInsert("AdsGroup")**. Diese Sichtbarkeitsbedingung wurde entfernt.	34544
An der Web Designer-Komponente **VI_ITShop_Approvals** wurden die folgenden Collections entfernt: • ITShopOrg • ITShopOrgForPWOToDecide • PWOHelperPWO • QERWorkingStep • PWOHelperPWOForRecallQuery An der Komponente **VI_ITShop_PWO_MasterDetail** wurde die Collection **ITShopOrg** entfernt.	201868
Im Web Portal wird beim automatischen Abbestellen von Produkten durch eine abgelehnte Attestierung eine falsche Begründung hinterlegt.	202027
Unter bestimmten Umständen kann ein Genehmiger eines Attestierungsfalls im Web Portal keine Analyse des Berechtigungsentzugs durchführen.	202031
Im Web Portal für Betriebsunterstützung können Benutzer für sich selbst Zugangscodes erstellen.	202046
Im Web Designer Web Portal ist es möglich, Hyperviews anzuzeigen, für die man nicht benötigten Berechtigungen besitzt.	223719
Der API Server lässt sich nicht installieren, da auf demselben Internet	227123

Gelöstes Problem	Fehler ID
Information Services ein WebDAV-Modul installiert ist.	
Wenn man im Web Portal nach AE/Ä sucht, werden auch Einträge mit A gefunden. HINWEIS: Führen Sie nach einer Update-Migration eine komplette Neuindizierung durch.	278865, 34389
Im Web Portal kommt es zu verlorenen ASP.NET-Sessions im Dauerbetrieb der Linux-Container.	34397
Identitäten mit der Berechtigungsgruppe **vi_4_PERSONADMIN** sehen im Web Portal nicht alle Bestellungen ihrer untergeordneten Identitäten.	33773
Wenn bei einer Abbestellung ein Abbestelldatum angegeben wird, das in der Vergangenheit liegt, erscheint im Web Portal eine Fehlermeldung. Anschließend kann das Produkt auch mit einem gültigen Datum nicht abbestellt werden.	34144
Im Web Portal ist es nicht möglich Compliance-Verletzungen aufzulösen, wenn die Verletzung eine Hauptidentität betrifft.	34416

Tabelle 7: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Mappings, bei denen die Option **Nicht für Neuanlage geeignet** aktiviert ist, verwenden die Verarbeitungsmethode `Insert`. Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#33217_001 und VPR#33217_002 bereitgestellt.	33217
Bei der Erkennung und Korrektur von unzulässigen Änderungen werden zu viele Einträge aufgezeichnet.	34439
Abbruch der Synchronisation durch Fehler bei der Synchronisation mit Revisionsfilterung: Der Typ der Revisionseigenschaft stimmt nicht überein. Fehlermeldung: `Error filtering by revision. ---> System.ArgumentException: Object must be of type Int32.`	34462
Fehler bei der Kompilierung von Skripten im C#-Syntax im Synchronization Editor, wenn bei einer Zuweisung ein Leerzeichen nach dem Gleichheitszeichen-Zeichen (**=**) fehlt.	34500
Fehler beim Erstellen eines Synchronisationsprojektes mit dem Kommandozeilenprogramm `SynchronizationEditor.CLI.exe`, wenn im Kennwort des Datenbankbenutzers ein Dollar-Zeichen (**$**) enthalten ist.	34531
Fehler beim Laden von Schemaklassen mit dem Klassentyp **Eindeutige Objekte** über das RemoteConnectPlugin.	34683
Fehler beim Provisionieren der Eigenschaft **Kennwort nicht änderbar** für Active Directory Benutzerkonten (`ADSAccount.UserCanNotChangePassword`).	34390

Gelöstes Problem	Fehler ID
Mangelnde Performance beim Öffnen von Zuweisungsformularen für `ADSAccountInADSGroup`.	34510
Die Azure AD Connect Anker-ID für Active Directory Benutzerkonten (`ADSAccount.MSDsConsistencyGuid`) ist im Mapping nicht schreibbar. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34715 bereitgestellt.	34715
Fehler beim Speichern eines Microsoft Exchange Postfachs, wenn die Eigenschaft **Kalenderautomatik aktiviert** (`EX0Mailbox.AutomateProcessing`) einen leeren Wert hat.	34610
Bei der automatischen Personenzuordnung wird für LDAP Benutzerkonten die Option **Gruppen erbbar** (`LDAPAccount.IsGroupAccount`) immer auf den Wert **True** gesetzt.	34556
Beim Löschen eines LDAP Benutzerkontos werden Mitgliedschaften in LDAP Gruppen nicht entfernt, wenn der Merge-Modus aktiv ist.	34594, 34601
Fehler im SCIM Konnektor bei der OAuth-Authentifizierung mit Benutzernamen und Kennwort. Fehlermeldung: `Fehler 400 BadRequest ({"error":"invalid_request","error_description":"The request contains invalid parameters or values."})`	34578
Fehler der Ausführung der Prozedur `EBS_UserInResp`. Fehlermeldung: `Conversion failed when converting date and/or time from character string.`	34754
Im SAP Konnektor wird das Property `LANGU` am Schematyp `SAPTSAD3T` nicht korrekt ausgegeben.	34557
Die Synchronisation versucht Zuweisungen von SAP Rollen an Benutzerkonten mit `XIsInEffect=0` im One Identity Manager nochmals zu erzeugen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34563 bereitgestellt.	34563
Suchkriterien für die automatische Personenzuordnung mit einer Oder-Verknüfung führen zu vielen Treffern, wenn eines der beteiligten Felder leer ist.	34415
Beim Ändern des Gültigkeitszeitraums werden Zuweisungen von SAP Rollen an Benutzerkonten vorübergehend gelöscht.	34577
Probleme bei der Synchronisation einer SharePoint Online-Umgebung, wenn im Zielsystem eine Websitesammlung (`Site`) umbenannt wurde.	34471
Die Definition eines Hierarchiefilters im Scope der One Identity Manager	32595

Gelöstes Problem	Fehler ID
Verbindung bringt falsche Ergebnisse.	
Nach Änderung der Aliasse an einem Google Workspace Benutzerkonto wird durch die Provisionierung der alte Wert zurückgelesen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34645 bereitgestellt.	34645
Bei der Initialsynchronisation wird das Internetkennwort von Notes Benutzerkonten eingelesen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34393 bereitgestellt.	34393
In Synchronisationsprojekten für Notes Domänen hat die Variable `MailFileAccessType` einen falschen Standardwert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#25230 bereitgestellt.	25230
In Synchronisationsprojekten für Unix-basierte Zielsysteme wird das Kennwort des Benutzers nicht verschlüsselt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#32500 bereitgestellt.	32500

Tabelle 8: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Falsche Bezeichnung in der Bitmasken-Konfiguration für `PersonHasObject.InheritInfo`.	34721
Bei der Abfrage der Herkunft von Berechtigungen kann es unter Umständen zu Blockaden kommen.	34767
Bei Deaktivierung einer Person werden geschlossene Attestierungsvorgänge nochmals geschlossen.	34665
Die Suche nach bestimmten Attestierungsvorgängen im Web Portal findet mitunter kein Ergebnis, wenn Systemberechtigungen attestiert werden. Ursache war die unterschiedliche Bildung von Anzeigenamen für die Attestierungsobjekte. Für einige Tabellen, die im Unified Namespace abgebildet werden, wurde das Anzeigemuster geändert. Dadurch werden diese Objekte nun in Berichten oder Ansichten des Web Portals mit anderen Namen dargestellt.	34681
Wenn eine Entscheidungsebene mit mehreren Entscheidungsschritten den Timeout erreicht, wird mehrfach ein identischer Prozess generiert.	34571
E-Mail-Benachrichtigungen über die positive Entscheidung von Bestellungen nennen den falscher Entscheider.	34614
Ein Produkt kann nicht für mehrere unterschiedliche Arbeitsplätze bestellt werden, für die eine Person verantwortlich ist.	30069

Siehe auch:

- Schemaänderungen auf Seite 47
- Patches für Synchronisationsprojekte auf Seite 67

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
Nach einer Simulation im Manager sind Objekte unter Umständen im inkonsistentem Zustand. Wird ein Objekt während einer Simulation verändert, gespeichert und die Simulation beendet, so bleibt das Objekt im letzten Zustand der Simulation erhalten. Weitere Änderungen an dieser Objektinstanz können unter Umständen nicht gespeichert werden. Lösung: Laden Sie nach dem Beenden der Simulation das Objekt neu.	12753
Im Configuration Wizard können unzulässige Modulkombinationen ausgewählt werden. Dies führt erst bei Beginn der Schemainstallation zu Fehlern. Ursache: Der Configuration Wizard wurde direkt gestartet. Lösung: Verwenden Sie zur Installation der One Identity Manager Komponenten immer die `autorun.exe`. Damit ist sichergestellt, das keine unzulässigen Modulkombinationen ausgewählt werden.	25315
Schemaerweiterungen an einer Datenbanksicht vom Typ **View** (beispielsweise `Department`) mit einer Fremdschlüsselbeziehung auf eine Spalte einer Basistabelle (beispielsweise `BaseTree`) oder einer Datenbanksicht vom Typ **View** sind nicht zulässig.	27203
Fehler bei der Verbindung über einen Anwendungsserver, wenn der private Schlüssel des Zertifikates, mit dem die `VI.DB` ihre Session-Information zu	27793

Bekanntes Problem	Fehler ID
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.	
Fehler beim Auslösen von Ereignissen auf eine View , welche keine UID-Spalte als Primärschlüssel besitzt. Primärschlüssel für Objekte im One Identity Manager bestehen immer aus einer oder, bei M:N-Tabellen, zwei UID-Spalten. Dies ist eine Basisfunktionalität im System. Die Definition einer View, die als Primärschlüssel den `XObjectKey` verwendet, ist nicht zulässig und wird an sehr vielen Stellen zu weiteren Fehlern führen. Zur Überprüfung des Schemas wird eine Konsistenzprüfung **Table of type U or R with wrong PK definition** bereitgestellt.	29535
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`	26739

Bekanntes Problem	Fehler ID
`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.	
Die Bestelleigenschaften eines Produktes werden bei der Verlängerung oder Abbestellung im Web Portal nicht aus der ursprünglichen Bestellung in den Warenkorb übernommen. Ursache: Bestelleigenschaften können in unterschiedlichen, kundenspezifischen Spalten gespeichert werden. Lösung: Erstellen Sie eine Bildungsregel für die (kundenspezifische) Spalte an der Tabelle `ShoppingCartItem`, in der die Bestelleigenschaft bei der Bestellung gespeichert wird. Diese Bildungsregel muss die Bestelleigenschaften für die verknüpfte Bestellung aus der identischen (kundenspezifischen) Spalte an der Tabelle `PersonWantsOrg` auslesen.	32364
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.
	33867

Bekanntes Problem	Fehler ID

• 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>`
`</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

Bekanntes Problem	Fehler ID
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
Synchronisationsprojekte für SAP R/3, die per Transport in eine One Identity Manager Datenbank importiert wurden, können nicht geöffnet werden. Das Problem tritt nur auf, wenn vor dem Import des Transportpakets noch kein SAP R/3 Synchronisationsprojekt in der Zieldatenbank angelegt wurde. Lösung: Erstellen und speichern Sie mindestens ein Synchronisationsprojekt für SAP R/3 in der Zieldatenbank, bevor Sie SAP R/3 Synchronisationsprojekte mit dem Database Transporter in diese Datenbank importieren.	27687
Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer Zentralen Benutzerverwaltung. Meldung: `No company is assigned.` Ursache: Für das Benutzerkonto konnte keine Firmenadresse ermittelt werden. Lösung: Stellen Sie sicher, dass entweder • jedem Benutzerkonto eine Firma zugeordnet ist, die im Zentralsystem existiert - ODER - • dem Zentralsystem eine Firma zugeordnet ist.	29253
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.	30271

Bekanntes Problem	Fehler ID
Workaround: Nutzen Sie den Manager, um den Zielsystemabgleich durchzuführen.	
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. - ODER - • Deaktivieren Sie den Cache in der Datei `VI.Projector.SharePoint.<Version>.Host.exe.config`.	31017
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.	32149

Bekanntes Problem	Fehler ID

Um die Typkonvertierung zu deaktivieren
• Fügen Sie folgende Einstellungen in die Datei `StdioProcessor.exe.config` ein.
  • In die vorhandene Sektion `<configSections>`:
  `<sectionGroup name="SAP.Middleware.Connector">`
  `<section name="GeneralSettings" type="SAP.Middleware.Connector.RfcGeneralConfiguration, sapnco, Version=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c7f7d23" />`
  `</sectionGroup>`
  • Eine neue Sektion:
  `<SAP.Middleware.Connector>`
  `<GeneralSettings anyDateTimeValueAllowed="true" />`
  `</SAP.Middleware.Connector>`	

Die in der Prozesskomponente `PowershellComponentNet4` im Parameter `OutputFile` zu erzeugende Datei enthält keine Fehlermeldungen. Ursache: In der Datei (Parameter `OutputFile`) werden keine Meldungen gesammelt. Die Datei dient als Exportdatei der in der Pipeline zurückgelieferten Objekte. Lösung: Die Ausgabe von Meldungen im Skript kann mittels *> Operator in eine im Skript festgelegte Datei erfolgen. Beispiel: `Write-Warning "Ich bin eine Meldung" *> "meldungen.txt"` Weiterhin werden Meldungen, die Mittels `Write-Warning` generiert werden, ebenfalls in die Protokolldatei des One Identity Manager Service geschrieben. Möchte man einen Abbruch mit Fehler im Skript erzwingen, so sollte man eine `Exception` werfen. Diese Meldung erscheint dann in der Protokolldatei des One Identity Manager Service.	32945
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	33104

Bekanntes Problem	Fehler ID
weiterhin benötigen. Ausführliche Informationen und ein Beispiel-XML finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Google Workspace-Umgebung*.	
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. 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

Tabelle 13: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
Unter SharePoint 2010 kann es zu einem Fehler bei der Synchronisation von SharePoint Websites kommen. Die Methode `SPWeb.FirstUniqueRoleDefinitionWeb()` löst eine `ArgumentException` aus. Weitere Informationen finden Sie unter https://support.microsoft.com/de-	24626

Bekanntes Problem	Fehler ID
de/kb/2863929.	
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: • Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 Uns ist derzeit nicht bekannt, ob weitere Windows Updates zu diesem Fehler führen können. Der Active Directory Konnektor korrigiert dieses Fehlverhalten mit einem Workaround beim Aktualisieren der Mitgliederliste. Da dieser Workaround die Performance bei der Provisionierung von Active Directory Gruppen verschlechtern kann, wird er aus künftigen One Identity Manager Versionen wieder entfernt, sobald Microsoft diesen Fehler behoben hat.	30575
Unter Umständen kommt es im Report Editor zur Verwendung der falschen Sprache in den Steuerelementen von Stimulsoft.	31155
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	31998

Bekanntes Problem	Fehler ID
Manager zu verschiedenen Problemen führen.	

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 8.1.5 zu Version 8.2.

Microsoft Teams Modul

- Neues Datenmodell für das Microsoft Teams Modul.

Application Governance Modul

- Neues Datenmodel für das Application Governance Modul.

Konfigurationsmodul

- Neue Tabelle `QBMColumnBitMaskConfig` und neue Spalten `DialogColumn.BitMaskConfigOrder`, `DialogColumn.DisallowCustomBitMaskConfig` und `DialogColumn.HasBitMaskConfig` zur Abbildung von Bitmasken.

- Neue Tabelle `QBMColumnLimitedValue` zur Abbildung von Listen zulässiger Werte.
- Neue Tabellen `QBMTableRevision` und `QBMVTableRevision` zur Abbildung von Revisionsdaten für Tabellen.
- Neue Tabelle `QBMTrustedSQL` und neue Spalte `QBMWebApplication.TrustedSourceKey` zur Abbildung von vertrauenswürdigen SQL Abfragen.
- Neue Tabelle `QBMVSystemState` zur Abbildung des Systemstatus.
- Neue Spalte `DialogColumn.MultiValueSpecification` zur Definition weiterer Anforderungen an die Einzelwerte von MVP-Spalten.
- Neue Spalten `DialogCountry.IsHistorical` und `DialogState.IsHistorical` zur Kennzeichnung von Ländern und Bundesländern als historisch.
- Neue Spalte `DialogDashBoardDef.DashBoardType` zur Abbildung von Typen von Statistikdefinitionen.
- Neue Spalte `DialogDatabase.UID_DialogCountryDefault` zur Angabe eines Standardlandes.
- Neue Spalte `DialogDatabase.UpdatePhase` zur Abbildung der Phasen für die stufenweise Vorbereitung einer Migration.
- Neue Spalte `DialogMethod.IsVisibleScript` für ein Skript zum bedingten Anzeigen der Methode.
- Neue Spalte `DialogRichMail.AttachmentFileName` als Vorlage zur Bildung des Dateinamens für den Berichtsanhang.
- Neue Spalte `DialogTable.DeleteDelayScript` für ein Skript zur Ermittlung einer objektspezifischen Löschverzögerung.
- Neue Spalte `DialogTable.SplittedLookupSupport` als Pfad zum Person-Objekt für tabellenübergreifende Suche.
- Neue Spalte `DialogTree.HelpKey` für die Abbildung eines Hilfeschlüssels.
- Neue Spalten für `QBMConsistencyCheck.AccessLevelMin`, `QBMConsistencyCheck.DescriptionElementDetect` und `QBMConsistencyCheck.DescriptionRepair` für Konsistenzprüfungen.
- Neue Spalten `QBMDBQueueTask.RestoreDelay` und `QBMDBQueueTaskPerf.RestoreDelay` zur Abbildung einer minimalen Zeit bis zur Reaktivierung von DBQueue Prozessor Aufträgen.
- Neue Spalten `QBMHtmlApp.Ident_QBMHtmlApp`, `QBMHtmlApp.IsPreCompiled` und `QBMHtmlApp.SortOrder` für HTML Anwendungen.
- Neue Spalten `QBMIdentityClient.AcrValues` und `QBMIdentityProvider.AcrValues` zur Abbildung von acr-Werten.
- Neue Spalten `QBMIdentityClient.IsSendPostLogoutRedirectURI` und `QBMIdentityClient.PostLogoutRedirectURI` für Angaben zur Weiterleitungs-URI.
- Neue Spalten `QBMIdentityClient.TokenEndpointCertThumbPrint` für den Fingerabdruck des Zertifikates zur Prüfung des Tokens.

- Neue Spalten `QBMIdentityProvider.CheckClaim` und `QBMIdentityProvider.CheckValue` Prüfung eines zusätzlichen Claim-Typs.
- Neue Spalte `QBMIdentityProvider.NoIdTokenCheck` zur Angabe, ob eine Prüfung des ID-Tokens stattfindet.
- Neue Spalte `QBMLimitedSQL.TypeOfLimitedSQL` zur Angabe eines Typs für das vordefinierte SQL.
- Neue Spalte `QBMPwdPolicy.MandatoryCharacterClasses` zu Angabe, wie viele Regeln für Zeichenklassen erfüllt sein müssen.
- Neue Spalten für `QBMServer.FQDNExternal`und `QBMServer.PortNumberExternal` für die Erreichbarkeit von Jobservern.
- Neue Spalte für `QBMServer.NotUsedForJobCreation` zur Angabe, ob der Jobserver an der Lastverteilung teilnimmt.
- Neue Spalte `QBMUniqueGroup.ViolationMessage` um Meldungstexte für Fehlermeldungen zu erfassen.
- Neue Spalte `QBMVSystemOverview.SubElement` für die bessere Auswertung der Systemkonfiguration.
- Der Datentyp für die Spalten `DialogColumnBulkDependencies.XTouched`, `QBMBufferConfig.XTouched`, `QBMColumnTranslation.XTouched`, `QBMNonLinearDepend.XTouched`, `QBMTransportHistory.XTouched` und `QBMUniqueGroupHasColumn.XTouched` wurde auf `nchar(1)` geändert.
- Die Spalte `DialogDatabase.ConnectionString` wurde auf `nvarchar(max)` verlängert.
- Die Spalte `DialogSchedule.StartTime` wurde auf `varchar(256)` verlängert.
- Die Spalte `QBMConsistencyCheck.Description` wurde auf `nvarchar(max)` verlängert.
- Die Spalten `QBMDBPrincipal.LoginName` und `QBMDBPrincipal.UserName` wurden auf `nvarchar(128)` verlängert.
- Die Spalte `QBMDBRoleDef.Rolename` wurde auf `nvarchar(400)` verlängert.
- Der Datentyp für die Spalte `QBMFileRevision.HashValue` wurde auf `varbinary (64)` geändert.
- Neue Pflichtfelddefinition für die Spalte `DialogObject.UID_DialogTable`.
- Die Tabelle `QBMVBlobInternal` wurde gelöscht.
- Die Spalte `QBMIdentityClient.TokenEndpointKey` wurde gelöscht.

Modul Zielsystemsynchronisation

- Neue Tabellen `DPRProjectionDependency` und `DPRSystemSyncDependency` zur Abbildung von Abhängigkeiten für die Synchronisation.
- Neue Tabellen `DPRVSyncRunMessages` und `DPRVSyncRunOverview` zur verbesserten Auswertung von Synchronisationsprotokollen.
- Neue Spalten zur Abbildung der Systemsynchronisation.

    - DialogColumn.SystemSyncDirection
    - DialogTable.SystemSyncKeyColumns
    - DialogTable.SystemSyncMode
    - DialogTable.UID_SystemSyncConfigCLRType
    - DPRProjectionConfigStep.DoNotRespectOutstanding
- Neue Spalte `DPRProjectionConfig.JournalMessageContexts` zur besseren Abbildung von Protokolleinträgen.
- Neue Spalten `DPRProjectionStartInfo.ProgressText` und `DPRProjectionStartInfo.ProgressValue` für die Abbildung des Fortschritts von Synchronisationen.
- Neue Spalte `DPRRevisionStore.ValueType` zur Abbildung der Art des Revisionswertes.
- Neue Spalte `DPRSchema.FunctionalLevel` zur Abbildung des Entwicklungsstandes eines Schemas.
- Neue Spalte `DPRSchemaType.ShrinkLock` um das Entfernen des Schematyps bei der Schemakompression zu verhindern.
- Neue Spalte `DPRShell.IsAutomaticallyManaged` zur Angabe, ob das Synchronisationsprojekt automatisch verwaltet wird.
- Neue Spalte `DPRShell.LastMigrationError` zur Abbildung der Fehlermeldung der letzten Migration eines Synchronisationsprojektes.
- Neue Spalte `DPRStartSequence.ConcurrConflHandling` zur Abbildung des Verhaltens bei Kollisionen.
- Neue Spalte `DPRStartSequenceHasProjection.CurrentJobReference` zur Abbildung des aktuell laufenden Prozesses.
- Die Spalte `DPRJournal.ProjectionState` wurde auf `varchar(64)` verlängert.
- Die Spalten `DPRSchemaProperty.AutoFillBehavior` und `DPRSchemaProperty.MandatoryBehavior` wurden auf `nvarchar(64)` verlängert.

Zielsystem Basismodul

- Neue Tabellen für die erweiterte Abbildung von Systemberechtigungen in Cloud Zielsystemen.
    - BaseTreeHasUNSGroupB1
    - BaseTreeHasUNSGroupB2
    - BaseTreeHasUNSGroupB3
    - DepartmentHasUNSGroupB1
    - DepartmentHasUNSGroupB2
    - DepartmentHasUNSGroupB3
    - ITShopOrgHasUNSGroupB1
    - ITShopOrgHasUNSGroupB2

    - ITShopOrgHasUNSGroupB3
    - ITShopSrcHasUNSGroupB1
    - ITShopSrcHasUNSGroupB2
    - ITShopSrcHasUNSGroupB3
    - LocalityHasUNSGroupB1
    - LocalityHasUNSGroupB2
    - LocalityHasUNSGroupB3
    - OrgHasUNSGroupB1
    - OrgHasUNSGroupB2
    - OrgHasUNSGroupB3
    - ProfitCenterHasUNSGroupB1
    - ProfitCenterHasUNSGroupB2
    - ProfitCenterHasUNSGroupB3
    - UNSAccountBHasUNSGroupB
    - UNSAccountBHasUNSGroupB1
    - UNSAccountBHasUNSGroupB2
    - UNSAccountBHasUNSGroupB3
    - UNSAccountBInUNSGroupB1
    - UNSAccountBInUNSGroupB2
    - UNSAccountBInUNSGroupB3
    - UNSGroupB1
    - UNSGroupB1Collection
    - UNSGroupB1Exclusion
    - UNSGroupB1InUNSGroupB1
    - UNSGroupB2
    - UNSGroupB2Collection
    - UNSGroupB2Exclusion
    - UNSGroupB2InUNSGroupB2
    - UNSGroupB3
    - UNSGroupB3Collection
    - UNSGroupB3Exclusion
    - UNSGroupB3InUNSGroupB3
- Neue Spalten `UNSRootB.GroupUsageMask`, `UNSRootB.UserContainsGroupList` und `UNSAccountB.XDateSubItem` für die erweiterte Abbildung von Systemberechtigungen in Cloud Zielsystemen.

- Neue Spalte `UNSGroupB.HasReadOnlyMemberships` zur Abbildung von dynamischen Mitgliedschaften.
- Neue Spalten `UNSAccountB.IsGroupAccount_UNSGroupB`, `UNSAccountB.IsGroupAccount_UNSGroupB1`, `UNSAccountB.IsGroupAccount_UNSGroupB2` und `UNSAccountB.IsGroupAccount_UNSGroupB3` zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten `UNSAccountB.IsNeverConnectManual` und `UNSAccountB.NeverConnectToPerson` zur Abbildung von Verbindungen zu Personen.
- Neue Spalte `AERoleHasTSBAccountDef.XIsInEffect` zur Abbildung der Wirksamkeit von Zuweisungen.
- Neue Spalte `TSBAERoleForRoot.UID_AERoleMemberShip` zur Abbildung von Zielsystemverantwortlichen.
- Neue Spalte `UNSAccountB.XDateSubItem` zur Abbildung des Änderungsdatums für Abhängigkeiten.
- Neue Spalte `UNSRootB.DeleteDelayDays` zur Abbildung einer Löschverzögerung für kundendefinierte Zielsysteme.
- Der Datentyp für die Spalten `UNSAccountB.MatchPatternForMembership` und `UNSGroupB.MatchPatternForMembership` wurde auf `bigint` geändert.
- Der Datentyp für die Spalten `TSBITData.XTouched`, `TSBITDataMapping.XTouched`, `TSBVUNSDomain.XTouched` und `TSBVUNSRoot.XTouched` wurde auf `nchar(1)` geändert.

Azure Active Directory Modul

- Neue Tabellen `AADApplication` und `AADApplicationOwner` zur Abbildung von Azure Active Directory Anwendungen.
- Neue Tabellen `AADServicePrincipal` und `AADServicePrincipalOwner` zur Abbildung von Azure Active Directory Dienstprinzipalen.
- Neue Tabellen `AADAppRole` und `AADAppRoleAssignment` zur Abbildung von App-Rollen.
- Neue Tabellen `AADGroupHasDeniedService`, `AADGroupHasSubSku` und `AADUserHasSubSkuCompressed` zur Abbildung der Lizenzzuweisungen über Azure Active Directory Gruppen.
- Neue Tabellen `AADHomeRealmDiscoveryPolicy`, `AADServicePrincipalOwner`, `AADTokenIssuancePolicy` und `AADTokenLifetimePolicy` zur Abbildung von Azure Active Directory Richtlinien.
- Neue Spalten zur Abbildung zusätzlicher Eigenschaften für Azure Active Directory Benutzerkonten.
    - AADUser.AboutMe
    - AADUser.AgeGroup
    - AADUser.BirthDay
    - AADUser.ConsentProvidedForMinor
    - AADUser.EmployeeID

    - AADUser.FaxNumber
    - AADUser.HireDate
    - AADUser.ImAddresses
    - AADUser.Interests
    - AADUser.IsResourceAccount
    - AADUser.LegalAgeGroupClassification
    - AADUser.MySite
    - AADUser.OnPremisesDistinguishedName
    - AADUser.OnPremisesDomainName
    - AADUser.OnPremisesExtensionAttribute1
    - AADUser.OnPremisesExtensionAttribute10
    - AADUser.OnPremisesExtensionAttribute11
    - AADUser.OnPremisesExtensionAttribute12
    - AADUser.OnPremisesExtensionAttribute13
    - AADUser.OnPremisesExtensionAttribute14
    - AADUser.OnPremisesExtensionAttribute15
    - AADUser.OnPremisesExtensionAttribute2
    - AADUser.OnPremisesExtensionAttribute3
    - AADUser.OnPremisesExtensionAttribute4
    - AADUser.OnPremisesExtensionAttribute5
    - AADUser.OnPremisesExtensionAttribute6
    - AADUser.OnPremisesExtensionAttribute7
    - AADUser.OnPremisesExtensionAttribute8
    - AADUser.OnPremisesExtensionAttribute9
    - AADUser.OnPremisesSAMAccountName
    - AADUser.OnPremisesUserPrincipalName
    - AADUser.OtherMails
    - AADUser.PastProjects
    - AADUser.PreferredName
    - AADUser.Responsibilities
    - AADUser.Schools
    - AADUser.Skills
- Neue Spalten `AADUser.ExternalUserState` und `AADUser.ExternalUserStateChangeDate` für die Abbildung von Gastbenutzern.

- Neue Spalten AADUser.NeverConnectToPerson und AADUser.IsNeverConnectManual zur Abbildung von Verbindungen zu Personen.
- Neue Spalten AADUser.IsGroupAccount_DeniedService, AADUser.IsGroupAccount_DirectoryRole, AADUser.IsGroupAccount_Group und ADUser.IsGroupAccount_SubSku zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalte AADUser.LastPasswordChangeDateTime zur Abbildung des Datums der letzten Kennwortänderung.
- Der Datentyp für die Spalten AADDeniedServicePlan.MatchPatternForMembership, AADDirectoryRole.MatchPatternForMembership, AADGroup.MatchPatternForMembership, AADSubSku.MatchPatternForMembership und AADUser.MatchPatternForMembership wurde auf bigint geändert.
- Die Pflichtfelddefinition für die Spalten AADUser.DisplayName und AADUser.UserPrincipalName wurde geändert.
- Die Tabelle AADSubSkuExclusion wurde gelöscht.
- Die Spalten AADUserHasSubSku.RiskIndexCalculated und AADUserHasSubSku.UID_AADSubSku wurden gelöscht.

Exchange Online Modul

- Neue Spalte AADUser.IsGroupAccount_UnifiedGroup zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten O3EMailbox.UID_Person, O3EMailbox.IsNeverConnectManual, O3EMailbox.NeverConnectToPerson, O3EMailContact.IsNeverConnectManual, O3EMailContact.NeverConnectToPerson, O3EMailUser.IsNeverConnectManual und O3EMailUser.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Neue Spalte O3EUnifiedGroup.HiddenFromExchClientsEnabled um die Office 365 Gruppe in Outlook auszublenden.
- Der Datentyp für die Spalten O3EDL.MatchPatternForMembership, O3EMailbox.MatchPatternForMembership, O3EMailContact.MatchPatternForMembership, O3EMailUser.MatchPatternForMembership und O3EUnifiedGroup.MatchPatternForMembership wurde auf bigint geändert .
- Der Datentyp für die Spalte O3EMailbox.XTouched wurde auf nchar(1) geändert.

Active Directory Modul

- Neue Spalten ADSAccount.IsNeverConnectManual, ADSAccount.NeverConnectToPerson, ADSContact.IsNeverConnectManual und ADSContact.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Neue Spalten ADSAccount.IsProtectedFromAccidentalDel, ADSContact.IsProtectedFromAccidentalDel, ADSGroup.IsProtectedFromAccidentalDel und ADSMachine.IsProtectedFromAccidentalDel zum Schutz vor versehentlichem Löschen.

- Neue Spalten ADSContact.MSDsConsistencyGuid, ADSGroup.MSDsConsistencyGuid und ADSMachine.MSDsConsistencyGuid zur Abbildung der Azure AD Connect Anker-ID.
- Neue Spalte ADSAccount.MiddleName zur Abbildung des zweiten Vornamens.
- Neue Spalte ADSGroup.HasReadOnlyMemberships zur Abbildung von dynamischen Mitgliedschaften.
- Der Datentyp für die Spalten ADSAccount.MatchPatternForMembership, ADSContact.MatchPatternForMembership und ADSGroup.MatchPatternForMembership wurde auf bigint geändert.

Active Roles Modul

- Neue Spalte ADSGroup.edsaIsDynamicGroup zur Abbildung dynamischer Gruppen.
- Neue Spalten ADSGroup.edsvaCGisControlledGroup und ADSGroup.edsvaGFIsGroupFamily zur Abbildung von Active Roles Group Family-Gruppen.

Microsoft Exchange Modul

- Neue Tabelle EX0AddrBookPolicy und neue Spalte EX0MailBox.UID_EX0AddrBookPolicy zur Abbildung von Microsoft Exchange Adressbuchrichtlinien.
- Neue Tabellen EX0MailboxFullAccessPerm und EX0MailboxSendAsPerm zur Abbildung von zusätzlichen Microsoft Exchange Postfachberechtigungen.
- Neue Spalten EX0MailBox.IsNeverConnectManual, EX0MailBox.NeverConnectToPerson, EX0MailContact.IsNeverConnectManual, EX0MailContact.NeverConnectToPerson, EX0MailUser.IsNeverConnectManual und EX0MailUser.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Neue Spalte EX0MailBox.IsSingleItemRecoveryEnabled für die Wiederherstellung einzelner Elemente.
- Neue Spalten EX0MailBoxDatabase.IsExcludedFromProvisioning und EX0MailBoxDatabase.IsSuspendedFromProvisioning zur Abbildung automatischen Postfachverteilung für Microsoft Exchange Postfachdatenbanken.
- Der Datentyp für die Spalten EX0DL.XTouched, EX0DynDL.XTouched, EX0MailBox.XTouched und EX0Server.XTouched wurde auf nchar(1) geändert.

Exchange Hybrid Modul

- Neue Spalten EXHRemoteMailbox.IsNeverConnectManual und EXHRemoteMailbox.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.

LDAP Modul

- Neue Spalten LDAPAccount.IsNeverConnectManual und LDAPAccount.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.

- Der Datentyp für die Spalten LDAPAccount.MatchPatternForMembership und LDAPGroup.MatchPatternForMembership wurde auf bigint geändert.
- Die Spalte LDPDomain.Ident_Domain wurde auf nvarchar(128) verlängert.

Modul Unix-basierte Zielsysteme

- Neue Spalten UNXAccount.IsNeverConnectManual und UNXAccount.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Der Datentyp für die Spalten UNXAccount.MatchPatternForMembership und UNXGroup.MatchPatternForMembership wurde auf bigint geändert.

Oracle E-Business Suite Modul

- Neue Spalten EBSUser.IsNeverConnectManual und EBSUser.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Der Datentyp für die Spalten EBSUser.MatchPatternForMembership und EBSResp.MatchPatternForMembership wurde auf bigint geändert.

Domino Modul

- Neue Spalten NDOUser.IsNeverConnectManual und NDOUser.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Der Datentyp für die Spalten NDOUser.MatchPatternForMembership und NDOGroup.MatchPatternForMembership wurde auf bigint geändert.

SharePoint Modul

- Neue Spalten SPSUser.IsGroupAccount_SPSGroup und SPSUser.IsGroupAccount_SPSRLAsgn zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten SPSUser.IsNeverConnectManual und SPSUser.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Der Datentyp für die Spalten SPSUser.MatchPatternForMembership, SPSRLAsgn.MatchPatternForMembership und SPSGroup.MatchPatternForMembership wurde auf bigint geändert.

SharePoint Online Modul

- Neue Tabelle O3SWebTemplate zur Abbildung von SharePoint Online Webvorlagen.
- Neue Spalten O3SUser.IsGroupAccount_Group und O3SUser.IsGroupAccount_RLAsgn zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten O3SUser.IsNeverConnectManual und O3SUser.NeverConnectToPerson zur Abbildung von Verbindungen zu Personen.
- Neue Spalten O3SSite.UserCodeWarningLevel zur Abbildung zusätzlicher Grenzwerte für SharePoint Online Websitesammlungen.

- Der Datentyp für die Spalten `O3SUser.MatchPatternForMembership`, `O3SRLAsgn.MatchPatternForMembership` und `O3SGroup.MatchPatternForMembership` wurde auf `bigint` geändert.

Google Workspace Modul

- Neue Tabellen zur Abbildung von Zuweisungen von Google Workspace Admin-Rollen.
  - DepartmentHasGAPOrgAdminRole
  - GAPBaseTreeHasOrgAdminRole
  - ITShopOrgHasGAPOrgAdminRole
  - ITShopSrcHasGAPOrgAdminRole
  - LocalityHasGAPOrgAdminRole
  - OrgHasGAPOrgAdminRole
  - ProfitCenterHasGAPOrgAdminRole
- Neue Spalten zur Abbildung von Zuweisungen von Google Workspace Admin-Rollen.
  - GAPOrgAdminRole.DisplayName
  - GAPOrgAdminRole.IsForITShop
  - GAPOrgAdminRole.IsITShopOnly
  - GAPOrgAdminRole.MatchPatternForMembership
  - GAPOrgAdminRole.RiskIndex
  - GAPOrgAdminRole.UID_AccProduct
  - GAPUserInOrgAdminRole.RiskIndexCalculated
  - GAPUserInOrgAdminRole.XIsInEffect
  - GAPUserInOrgAdminRole.XOrigin
- Neue Spalten `GAPUser.IsGroupAccount_Group`, `GAPUser.IsGroupAccount_OrgAdminRole` und `GAPUser.IsGroupAccount_PaSku` zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten `GAPUser.IsNeverConnectManual` und `GAPUser.NeverConnectToPerson` zur Abbildung von Verbindungen zu Personen.
- Neue Spalten zur Abbildung zusätzlicher Eigenschaften für Google Workspace Benutzerkonten.
  - GAPUser.GenderAddressMeAs
  - GAPUser.GenderCustomGender
  - GAPUser.GenderType
  - GAPUser.RecoveryEmail
  - GAPUser.RecoveryPhone
- Neue Spalten zur Abbildung zusätzlicher Eigenschaften für Google Workspace Gruppen.

    - GAPGroup.stWhoCanContactOwner
    - GAPGroup.stWhoCanDiscoverGroup
    - GAPGroup.stWhoCanModerateContent
    - GAPGroup.stWhoCanModerateMembers
    - GAPGroup.stWhoCanViewGroup
    - GAPGroup.stWhoCanViewMembership
- Der Datentyp für die Spalten `GAPGroup.MatchPatternForMembership`, `GAPPaSku.MatchPatternForMembership` und `GAPUser.MatchPatternForMembership` wurde auf `bigint` geändert.
- Die Spalten `GAPGroup.stAllowGoogleCommunication` und `GAPGroup.stShowInGroupDirectory` wurden gelöscht.

SAP R/3 Benutzermanagement-Modul

- Neue Spalten `SAPUser.IsGroupAccount_SAPGrp`, `SAPUser.IsGroupAccount_SAPProfile` und `SAPUser.IsGroupAccount_SAPRole` zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten `SAPUser.IsNeverConnectManual` und `SAPUser.NeverConnectToPerson` zur Abbildung von Verbindungen zu Personen.
- Neue Spalte `SAPUser.IdAdType` zur Abbildung von Benutzertypen.
- Neue Spalten zur Abbildung zusätzlicher Eigenschaften für SAP Benutzerkonten.
    - SAPUser.BirthName
    - SAPUser.FirstName2
    - SAPUser.LastName2
    - SAPUser.NameAddOn
    - SAPUser.NameAddOn2
    - SAPUser.SORT1
    - SAPUser.SORT2
- Der Datentyp für die Spalten `SAPGroup.MatchPatternForMembership`, `SAPGrp.MatchPatternForMembership`, `SAPProfile.MatchPatternForMembership`, `SAPRole.MatchPatternForMembership` und `SAPUser.MatchPatternForMembership` wurde auf `bigint` geändert.

Modul SAP R/3 Compliance Add-on

- Neue Tabelle `SACTransactionType` und neue Spalten `SAPTransaction.UID_SACTransactionType` und `SAPFunctionDetail.UID_SACTransactionType` zur Abbildung von SAP Applikationstypen.
- Neue Spalten zur Abbildung zusätzlicher Eigenschaften für Funktionsdefinition.

    - SAPFunctionDetail.AUTHOBJNAM
    - SAPFunctionDetail.AUTHOBJTYP
    - SAPFunctionDetail.AUTHPGMID
    - SAPFunctionDetail.RFC_NAME
    - SAPFunctionDetail.RFC_TYPE
    - SAPFunctionDetail.SAPHashValue
    - SAPFunctionDetail.SRV_NAME
    - SAPFunctionDetail.SRV_TYPE
    - SAPFunctionDetail.TCD
- Neue Spalten zur Abbildung zusätzlicher Eigenschaften für SAP Applikationen.
    - SAPTransaction.AUTHOBJNAM
    - SAPTransaction.AUTHOBJTYP
    - SAPTransaction.AUTHPGMID
    - SAPTransaction.RFC_NAME
    - SAPTransaction.RFC_TYPE
    - SAPTransaction.SAPHashValue
    - SAPTransaction.SimpleCompareProperty
    - SAPTransaction.SRV_NAME
    - SAPTransaction.SRV_TYPE
    - SAPTransaction.TCD
    - SAPTransaction.TransactionDisplay
    - SAPFunctionInstanceDetail.UID_SAPTransaction
- Die Spalten `SAPFunctionDetail.TransactionCode`, `SAPFunctionInstanceDetail.TransactionCode` und `SAPTransaction.Ident_SAPTransaction` wurden gelöscht.

Modul SAP R/3 Strukturelle Profile Add-on

- Neue Spalte `SAPUser.IsGroupAccount_SAPHRP` zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Der Datentyp für die Spalte `SAPHRP.MatchPatternForMembership` wurde auf `bigint` geändert.

Privileged Account Governance Modul

- Neue Spalten zur Abbildung von Zugriffsanforderungen für SSH-Schlüssel für One Identity Safeguard.

    - PAGAsset.SSHHostKeyFingerPrint
    - PAGAsset.SSHKeyProfileName
    - PAGAstAccount.AllowSSHKeyRequest
    - PAGAstAccount.HasSSHKey
    - PAGAstAccount.SSHKeyProfileName
    - PAGUserAttestation.AllowSSHKeyRequest
- Neue Spalte `PAGUser.AllowPersonalAccounts` zur Unterstützung des Vault für persönliche Kennwörter.
- Neue Spalten `PAGUser.IsNeverConnectManual` und `PAGUser.NeverConnectToPerson` zur Abbildung von Verbindungen zu Personen.
- Der Datentyp für die Spalten `PAGUser.MatchPatternForMembership` und `PAGUsrGroup.MatchPatternForMembership` wurde auf `bigint` geändert.
- Der Datentyp für die folgenden Spalten wurde auf `nchar(1)` geändert.
    - PAGAccessOrder.XTouched
    - PAGAccGroup.XTouched
    - PAGAccGroupHasMember.XTouched
    - PAGAppliance.XTouched
    - PAGAsset.XTouched
    - PAGAssetInAstGroup.XTouched
    - PAGAstAccount.XTouched
    - PAGAstGroup.XTouched
    - PAGDirAccount.XTouched
    - PAGDirectory.XTouched
    - PAGEntl.XTouched
    - PAGEntlHasMember.XTouched
    - PAGIdentityProvider.XTouched
    - PAGReqPolicy.XTouched
    - PAGReqPolicyApprover.XTouched
    - PAGReqPolicyHasDirAccount.XTouched
    - PAGReqPolicyReviewer.XTouched
    - PAGReqPolicyScopeItem.XTouched
    - PAGUser.XTouched
    - PAGUserAttestation.XTouched
    - PAGUserHasDirAccount.XTouched

    - PAGUserInUsrGroup.XTouched
    - PAGUsrGroup.XTouched

Modul Cloud Systems Management

- Neue Tabellen für die erweiterte Abbildung von Systemberechtigungen in Cloud Zielsystemen.
    - CSMBaseTreeHasGroup1
    - CSMBaseTreeHasGroup2
    - CSMBaseTreeHasGroup3
    - CSMGroup1
    - CSMGroup1Collection
    - CSMGroup1Exclusion
    - CSMGroup1InGroup1
    - CSMGroup2
    - CSMGroup2Collection
    - CSMGroup2Exclusion
    - CSMGroup2InGroup2
    - CSMGroup3
    - CSMGroup3Collection
    - CSMGroup3Exclusion
    - CSMGroup3InGroup3
    - CSMUserHasGroup
    - CSMUserHasGroup1
    - CSMUserHasGroup2
    - CSMUserHasGroup3
    - CSMUserInGroup1
    - CSMUserInGroup2
    - CSMUserInGroup3
    - DepartmentHasCSMGroup1
    - DepartmentHasCSMGroup2
    - DepartmentHasCSMGroup3
    - ITShopOrgHasCSMGroup1
    - ITShopOrgHasCSMGroup2
    - ITShopOrgHasCSMGroup3
    - ITShopSrcHasCSMGroup1

    - ITShopSrcHasCSMGroup2
    - ITShopSrcHasCSMGroup3
    - LocalityHasCSMGroup1
    - LocalityHasCSMGroup2
    - LocalityHasCSMGroup3
    - OrgHasCSMGroup1
    - OrgHasCSMGroup2
    - OrgHasCSMGroup3
    - ProfitCenterHasCSMGroup1
    - ProfitCenterHasCSMGroup2
    - ProfitCenterHasCSMGroup3
- Neue Spalten `CSMRoot.GroupUsageMask` und `CSMRoot.UserContainsGroupList` für die erweiterte Abbildung von Systemberechtigungen in Cloud Zielsystemen.
- Neue Spalten `CSMUser.IsGroupAccount_CSMGroup`, `CSMUser.IsGroupAccount_CSMGroup1`, `CSMUser.IsGroupAccount_CSMGroup2` und `CSMUser.IsGroupAccount_CSMGroup3` zur besseren Abbildung der Vererbung von Gruppen und von Berechtigungen.
- Neue Spalten `CSMUser.NeverConnectToPerson` und `CSMUser.IsNeverConnectManual` zur Abbildung von Verbindungen zu Personen.
- Neue Spalte `CSMRoot.DeleteDelayDays` zur Abbildung einer Löschverzögerung für Cloud Zielsysteme.
- Der Datentyp für die Spalten `CSMUser.MatchPatternForMembership` und `CSMGroup.MatchPatternForMembership` wurde auf `bigint` geändert.

Modul Universal Cloud Interface

- Neue Tabellen für die erweiterte Abbildung von Systemberechtigungen in Cloud Zielsystemen.
    - UCIGroup1
    - UCIGroup1InGroup1
    - UCIGroup2
    - UCIGroup2InGroup2
    - UCIGroup3
    - UCIGroup3InGroup3
    - UCIUserHasGroup
    - UCIUserHasGroup1
    - UCIUserHasGroup2
    - UCIUserHasGroup3

    - UCIUserInGroup1
    - UCIUserInGroup2
    - UCIUserInGroup3
- Neue Spalten `UCIRoot.GroupUsageMask` und `UCIRoot.UserContainsGroupList` und `UCIUser.XDateSubItem` für die erweiterte Abbildung von Systemberechtigungen in Cloud Zielsystemen.

Identity Management Basismodul

- Neue Tabellen `QERPickCategory` und `QERPickedItem` für die Stichprobenattestierung.
- Neue Tabelle `DynamicGroupHasImmediateColumn` und neue Spalten `DynamicGroup.IsCalculateImmediately` und `DynamicGroup.IsRecalculationDeactivated` für die verbesserte Berechnung von dynamischen Rollen.
- Neue Tabelle `QERDynamicGroupBlackList` zur Abbildung von Ausschlusslisten für dynamischen Rollen.
- Neue Tabelle `QERBufferRecalcDecisionMaker` zur verbesserten Berechnung von Entscheidern.
- Neue Tabelle `QERITShopOwnerUsage` zur Abbildung von Produkteigentümern.
- Neue Tabellen `QERUniversalSubstitute` und `QERUniversalSubstituteInRoot` zur verbesserten Abbildung von Delegierungen.
- Neue Tabellen `QERVBaseTreeHasElement` und `QERVPersonHasElement` zur Zusammenfassung von Zuweisungen.
- Neue Tabelle `QERVFirstUnicodeChar` zur Verbesserung der Gruppierung und Filterung von Objekten nach Namen.
- Neue Spalten zur Abbildung einer Anwendungsrolle für Manager von Unternehmensstrukturen.
    - AERole.UID_AERoleManager
    - BaseTree.UID_AERoleManager
    - Department.UID_AERoleManager
    - ITShopOrg.UID_AERoleManager
    - ITShopSrc.UID_AERoleManager
    - Locality.UID_AERoleManager
    - ProfitCenter.UID_AERoleManager
- Neue Spalten für die Abbildung von Begründungen für Entscheidungen.
    - AccProduct.ApproveReasonType
    - AccProduct.DenyReasonType
    - AccProduct.OrderReasonType
    - AccProductGroup.ApproveReasonType

    - AccProductGroup.DenyReasonType
    - AccProductGroup.OrderReasonType
    - PWODecisionStep.ApproveReasonType
    - PWODecisionStep.DenyReasonType
- Neue Spalte `AccProductParamCategory.IsOldStyle` als Kennzeichen, ob für die Bestellparameter dieser Bestelleigenschaft die veraltete Definition genutzt wird.
- Neue Spalten `QERWorkingStep.EscalateIfNoApprover` und `PWODecisionStep.EscalateIfNoApprover` für die verbesserte Eskalation.
- Neue Spalte `PersonWantsOrg.UiOrderState` zur Anzeige des Status der Bestellung im Web Portal.
- Neue Spalte `PWODecisionRuleRulerDetect.SQLQueryObjectsToRecalc` zur verbesserten Neuberechnung der Entscheider.
- Neue Spalte `AERoleHasQERResource.XIsInEffect` zur Abbildung der Wirksamkeit von Zuweisungen.
- Neue Spalten `OrgRoot.IsPersonAssignOnce` und `OrgType.IsPersonAssignOnce` um die Zuweisung von Personen an mehrere Unternehmensstrukturen zu verhindern.
- Neue Spalte `Person.DecentralizedIdentifier` zur Abbildung eine dezentralen Identität.
- Neue Spalte `Person.IsPwdResetByHelpdeskAllowed` zur Angabe, ob das Zurücksetzen des Kennwortes durch Mitarbeiter des Kennwort-Helpdesk erlaubt ist.
- Neue Spalten `QERAssign.IsMAllAssign`, `ShoppingCartItem.ObjectKeyElementUsedInAssign` und `ShoppingCartItem.ObjectKeyOrgUsedInAssign` zur Unterstützung von Zuweisungsbestellungen für Ressourcen.
- Die Spalte `QERAssign.Ident_QERAssign` wurde auf `nvarchar(256)` verlängert.
- Der Datentyp der Spalte `PersonPasswordHistory.XTouched` wurde auf `nchar(1)` geändert.

Modul Attestierung

- Neue Spalten `AttestationCase.IsUnderConstruction` und `AttestationRun.CountChunksUnderConstruction` als Kennzeichen, dass die Erstellung des Attestierungsvorgangs ist noch nicht abgeschlossen.
- Neue Spalten `AttestationObject.UiText`, `AttestationObject.UiTextGrouped1`, `AttestationObject.UiTextGrouped2` und `AttestationObject.UiTextGrouped3` zur Abbildung von Textvorlagen für Attestierungsverfahren.
- Neue Spalten `AttestationPolicy.IsSetApprovalStateOnApproved` und `AttestationPolicy.IsSetApprovalStateOnDenied` zum automatischen Setzen des Zertifizierungsstatus.
- Neue Spalte `AttestationPolicy.IsShowElementsInvolved` um die zu attestierenden Objekte anzuzeigen.

- Neue Spalte `AttestationPolicy.UID_DialogCulture` zur Abbildung der Sprache, in der zu attestierende Informationen angezeigt werden.
- Neue Spalte `AttestationPolicy.UID_AERoleOwner` zur Abbildung einer Anwendungsrolle, deren Mitglieder die Attestierungsrichtlinie bearbeiten dürfen.
- Neue Spalten `AttestationPolicy.UID_QERPickCategory` und `AttestationWizardParm.UID_DialogTablePickCategory` für die Stichprobenattestierung.

Modul Complianceregeln

- Neue Spalte `ComplianceRule.UID_DialogRichMailNewViolation` für die Mailvorlage für neue Regelverletzungen.
- Neue Spalte `PersonInNCHasMControl.IsInActive` und `PersonInNCHasMControl.UID_PersonWantsOrg` zur verbesserten Zuweisung von risikomindernden Maßnahmen während der Genehmigung von Bestellungen.

Modul Unternehmensrichtlinien

- Neue Spalte `QERPolicy.UID_DialogDashBoardDef` zur Abbildung von Statistiken für Richtlinienverletzungen.
- Neue Spalte `QERPolicy.UID_DialogReport` zur Abbildung von Berichten für Richtlinienverletzungen.
- Neue Spalte `QERPolicy.UID_DialogRichMailNewViolation` für die Mailvorlage für neue Richtlinienverletzungen.

Geschäftsrollenmodul

- Neue Spalte `Org.UID_AERoleManager` zur Abbildung einer Anwendungsrolle für Manager von Geschäftsrollen.

Modul Berichtsabonnement

- Neue Spalte `AERoleHasRPSReport.XIsInEffect` zur Abbildung der Wirksamkeit von Zuweisungen.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 8.1.5 zu Version 8.2. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 96.

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 67.

Tabelle 14: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Azure Active Directory Modul	Azure Active Directory Synchronization	geändert
Active Directory Modul	Active Directory Synchronization	geändert
Active Roles Modul	Synchronize Active Directory Domain via Active Roles	geändert
Modul Cloud Systems Management	Universal Cloud Interface synchronization	keine
Oracle E-Business Suite Modul	Oracle E-Business Suite Synchronization	geändert
	Oracle E-Business Suite CRM data	geändert
	Oracle E-Business Suite HR data	geändert
	Oracle E-Business Suite OIM data	geändert
Microsoft Exchange Modul	Microsoft Exchange 2013_2016 Synchronization (v2)	geändert
	Microsoft Exchange 2013 / 2016 Synchronization (abgekündigt)	geändert
	Microsoft Exchange 2010 Synchronization (v2)	geändert
Google Workspace Modul	Google Workspace Synchronization	geändert
LDAP Modul	AD LDS Synchronization	geändert
	AD LDS Synchronization (version 2)	neu
	OpenDJ Synchronization	geändert
	OpenDJ Synchronization (version 2)	neu
	Generic LDAP Synchronization (version 2)	neu
	Oracle DSEE Synchronization (version 2)	neu
Domino Modul	Lotus Domino synchronization	geändert
Exchange Online Modul	Exchange Online Synchronization (v2)	geändert

Modul	Synchronisationsvorlage	Art der Änderung
Privileged Account Governance Modul	One Identity Safeguard Synchronization	geändert
SAP R/3 Benutzermanagement-Modul	SAP R/3 Synchronization (Base Administration)	geändert
	SAP R/3 (CUA subsystem)	geändert
Modul SAP R/3 Analyseberechtigungen Add-on	SAP R/3 BW	geändert
Modul SAP R/3 Compliance Add-on	SAP R/3 authorization objects	geändert
Modul SAP R/3 Strukturelle Profile Add-on	SAP R/3 HCM authentication objects	geändert
	SAP R/3 HCM employee objects	geändert
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	geändert
	AIX Account Management	geändert
Modul Zielsystemsynchronisation	Automatic One Identity Manager synchronization	neu

Patches für Synchronisationsprojekte

Im One Identity Manager 8.2 werden Patches für folgende Patchtypen bereitgestellt:

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

Um bestehende Synchronisationsprojekte an die One Identity Manager Version 8.2 anzupassen, müssen die Meilensteine angewendet werden. Je Kontext wird ein Meilenstein bereitgestellt. Ein Meilenstein fasst alle Patches für gelöste Probleme und die Meilensteine der Vorversionen zusammen, wenn diese noch nicht angewendet wurden. Sobald der aktuelle Meilenstein auf ein Synchronisationsprojekt angewendet wurde, ist dieses Synchronisationsprojekt mit dem One Identity Manager 8.2 kompatibel.

Patches für neue Funktionen können optional angewendet werden.

Nachfolgend finden Sie eine Liste der Patches für Synchronisationsprojekte, die im One Identity Manager 8.2 neu bereitgestellt werden. Es sind nur die Patches aufgelistet, die nach der Version 8.1.5 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 96.

Tabelle 15: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2	Meilenstein für den Kontext **DPR**".	
	Meilenstein 8.2	Meilenstein für den Kontext **One Identity Manager**.	

Tabelle 16: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#28669	Unterstützung von Einladungen von Gastbenutzern	Erweitert das Mapping `User` für die Erstellung von Gastbenutzern durch das Versenden von Einladungen.	28669
VPR#31389	Unterstützung von Schemaeigenschaften für Hybrid-Umgebungen, Altersgruppen und Benutzerprofilen	Fügt neue Property-Mapping-Regeln in das Mapping `User` ein, zur Unterstützung von Hybrid-Umgebungen, Altersgruppen und Benutzerprofilen.	31389
VPR#32384	Unterstützung von Lizenzzuweisungen über Azure Active Directory Gruppen	Erweitert die Synchronisationskonfiguration zur Unterstützung von Lizenzzuweisungen über Azure Active Directory Gruppen.	32384
VPR#32454	Setzt das Schlagwort **AzureAD** an Synchronisationsprojekten	Setzt das Schlagwort **AzureAD** an Synchronisationsprojekten für Azure Active Directory.	32454
VPR#32665	Synchronisation von	Fügt Property-Mapping-Regeln	32665

Patch ID	Patch	Beschreibung	Fehler ID
	`ExternalUserState` und `ExternalUserState-ChangeDateTime`	für die Schemaeigenschaften `ExternalUserState` und `ExternalUserStateChange-DateTime` in das Mapping `User` ein.	
VPR#32975	Hinzufügen einer Property-Mapping-Regel für `LastPasswordChangeDate-Time`	Fügt eine Property-Mapping-Regel für `LastPasswordChangeDateTime` in das Mapping `User` ein.	32975
VPR#33088	Unterstützung für Azure Active Directory Dienst-prinzipale	Erweitert die Synchro-nisationskonfiguration zur Unterstützung von Azure Active Directory Dienst-prinzipalen und App-Rollen. Voraussetzung für Patch **Unterstützung von Active Directory Richtlinien**.	33088
VPR#33198	Unterstützung von Active Directory Richtlinien	Erweitert die Synchro-nisationskonfiguration zur Unterstützung von Active Directory Richtlinien. Abhängig von Patch **Unter-stützung für Azure Active Directory Dienstprinzipale**.	33198
VPR#34150	Unterstützung von Microsoft Cloud for US Government (L4)	Fügt die Unterstützung für Microsoft Cloud for US Gover-nment (L4) ein.	34150
	Meilenstein 8.2	Meilenstein für den Kontext **Azure Active Directory**.	

Tabelle 17: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32110	Hinzufügen der Schemaei-genschaft `middleName`	Fügt die Schemaeigenschaft `middleName` in die Mappings `user` und `inetOrgPerson` ein.	32110
VPR#32759	Hinzufügen von Property-Mapping-Regeln für die Schemaeigenschaft `ProtectedFromAccidental-Deletion`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `ProtectedFromAccidental-Deletion` in die Mappings `user`, `contact`, `group` und	32759

Patch ID	Patch	Beschreibung	Fehler ID
		computer ein.	
VPR#32950	Hinzufügen weiterer Property-Mapping-Regeln für die Schemaeigenschaft mS-DS-ConsistencyGuid	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft mS-DS-ConsistencyGuid in die Mappings contact, group und computer ein. Voraussetzung für Patch **Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft mS-DS-ConsistencyGuid**.	32950
VPR#33217_001	Prüft die Eigenschaften von Mappings	Prüft und korrigiert Mappings, bei denen die Option **Nicht für Neuanlage geeignet** aktiviert ist.	33217
VPR#34324	Publizieren der Gruppenmitglieder als schreibgeschützt	Publizieren der Eigenschaften member von Gruppen als schreibgeschützt, um Schreibvorgänge im Zielsystembrowser zu vermeiden.	34324
VPR#34715	Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft mS-DS-ConsistencyGuid	Korrigiert die Mappingrichtung der Property-Mapping-Regel für die Schemaeigenschaft mS-DS-ConsistencyGuid im Mapping user. Abhängig von Patch **Hinzufügen weiterer Property-Mapping-Regeln für die Schemaeigenschaft mS-DS-ConsistencyGuid**.	34715
	Meilenstein 8.2	Meilenstein für den Kontext **Active Directory**.	

Tabelle 18: Patches für Active Roles

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32110	Neue Property-Mapping-	Fügt eine Property-Mapping-	32110

Patch ID	Patch	Beschreibung	Fehler ID
	Regel für `middleName`	Regel für die Schemaeigenschaft `middleName` in die Mappings `User` und `InetOrgPerson` ein.	
VPR#32783	Neue Property-Mapping-Regel für `edsvaProtectFromDeletion`	Fügt eine Property-Mapping-Regel für `edsvaProtectFromDeletion` in die Mappings `Group`, `Computer`, `User` und `InetOrgPerson` ein.	32783
VPR#32952	Hinzufügen von Property-Mapping-Regeln für `mS-DS-ConsistencyGuid`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `mS-DS-ConsistencyGuid` in die Mappings `Contact`, `Group`, `Computer`, `User` und `InetOrgPerson` ein.	32952
VPR#34168	Neue Property-Mapping-Regel für `edsaIsDynamicGoup`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `edsaIsDynamicGoup` in das Mapping `Group` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34168
VPR#34634	Neue Property-Mapping-Regeln für `edsvaGFIsGroupFamily` und `edsvaCGIsControlledGroup`	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `edsvaGFIsGroupFamily` und `edsvaCGIsControlledGroup` in das Mapping `Group` ein.	34634
	Meilenstein 8.2	Meilenstein für den Kontext **Active Roles**.	

Tabelle 19: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33804	Bereinigung von Verbindungsparametern	Entfernt nicht benötigte Parameter der Systemverbindung aus dem Verbindungsparameter.	33804

Patch ID	Patch	Beschreibung	Fehler ID
		Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 8.2	Meilenstein für den Kontext **Oracle E-Business Suite**.	

Tabelle 20: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#21073	Unterstützung der Postfachberechtigungen **Senden als** und **Vollzugriff**	Erweitert die Synchronisationskonfiguration zur Unterstützung der Postfachberechtigungen **Senden als** und **Vollzugriff**. HINWEIS: Da dies große Auswirkungen auf die Performance hat, sind die entsprechenden Synchronisationsschritte standardmäßig deaktiviert und müssen manuell aktiviert werden.	21073
VPR#26120	Neue Property-Mapping-Regeln für `IsExcludedFromProvisioning` und `IsSuspendedFromProvisioning`	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `IsExcludedFromProvisioning` und `IsSuspendedFromProvisioning` in das Mapping `MailboxDatabase` ein.	26120
VPR#27741	Unterstützung von Adressbuchrichtlinien	Erweitert die Synchronisationskonfiguration zur Unterstützung von Adressbuchrichtlinien für Postfächer.	27741
VPR#31470	Neue Property-Mapping-Regel für `IsSingleItemRecoveryEnabled`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `IsSingleItemRecoveryEnabled` in das Mapping `Mailbox` ein.	31470
	Meilenstein 8.2	Meilenstein für den Kontext **Microsoft Exchange**.	

Tabelle 21: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34170	Unterstützung von Microsoft Cloud for US Government (L4)	Fügt die Unterstützung für Microsoft Cloud for US Government (L4) ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34170
VPR#34046	Neue Property-Mapping-Regel für `HiddenFromExchangeClientsEnabled`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `HiddenFromExchangeClientsEnabled` im Mapping `UnifiedGroup` ein.	34046
	Meilenstein 8.2	Meilenstein für den Kontext **Exchange Online**.	

Tabelle 22: Patches für Google Workspace

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32610	Abbildung verschiedener Zugriffsberechtigungen von Gruppen	Erweitert das Mapping `Group` zur Abbildung von Zugriffsberechtigungen. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32610
VPR#33093	Abbildung zusätzlicher Schemaeigenschaften für Benutzerkonten	Erweitert das Mapping `User` zur Abbildung weiterer Schemaeigenschaften von Benutzerkonten.	33093
VPR#34645	Korrektur im Mapping `User`	Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft `Aliases` im Mapping `User`.	34645
	Meilenstein 8.2	Meilenstein für den Kontext **Google Workspace**.	

Tabelle 23: Patches für LDAP

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33513	Unterstützung	Erweitert den Scope und das	33513

Patch ID	Patch	Beschreibung	Fehler ID
	mehrerer Domänen mit dem gleichen DN	Standardvariablenset, um mehrere Domänen mit dem gleichen definierten Namen zu unterstützen.	
	Meilenstein 8.2	Meilenstein für den Kontext **LDAP**.	

Tabelle 24: Patches für HCL Domino

Patch ID	Patch	Beschreibung	Fehler ID
VPR#25230	Ändert den Standardwert der Variable `MailFileAccessType`	Ändert den Standardwert der Variable `MailFileAccessType` auf **0**.	25230
VPR#34393	Korrektur einer Property-Mapping-Regel im Mapping `Person`	Korrigiert Einstellungen der Property-Mapping-Regel für InternetPassword im Mapping `Person`. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34393
	Meilenstein 8.2	Meilenstein für den Kontext **HCL Domino**.	

Tabelle 25: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32541	Unterstützung von Zugriffsanforderungen für SSH-Schlüssel	Fügt Property-Mapping-Regeln in die Mappings `Asset` und `AssetAccount` ein, um Zugriffsanforderungen für SSH-Schlüssel zu unterstützen.	32541
VPR#34392	Unterstützung der Vault für persönliche Kennwörter	Fügt Property-Mapping-Regeln für die Schemaeigenschaft `AllowPersonalAccounts` ins Mapping `User` ein.	34392
VPR#34403	Behandlung von Kennwörtern als geheime Werte	Aktualisiert das Konnektorschema, um Kennwörter als geheime Werte zu behandeln. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34403

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2	Meilenstein für den Kontext **Privileged Account Management**.	

Tabelle 26: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33217_002	Prüft die Eigenschaften von Mappings	Prüft und korrigiert Mappings, bei denen die Option **Nicht für Neuanlage geeignet** aktiviert ist.	33217
VPR#33301	Unterstützung von SAP S/4HANA Nutzertypen und Kommunikationsdaten	Erweitert die Synchronisationskonfiguration zur Abbildung der Adress- und Kommunikationsdaten von Geschäftspartnern.	33301
VPR#33301_2	Unterstützung von SAP S/4HANA Nutzertypen	Erweitert die Synchronisationskonfiguration zur Abbildung von Nutzertypen.	33301
VPR#33819	Neu Property-Mapping-Regel für die Standardfirma von SAP Mandanten	Fügt eine Property-Mapping-Regel zur Abbildung der Standardfirma von SAP Mandanten in das Mapping `mandant` ein.	33819
VPR#34563	Korrektur von `userInRole` Mapping und Synchronisationsschritt	Korrigiert das Mapping und den Synchronisationsschritt für `SAPUserInSAPRole`-Zuweisungen, die nicht wirksam sind. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. Abhängig von Patch **Legt eine Schemaklasse für den Schematyp SAPUserInSAPRole an** (VPR#31427).	34563
	Meilenstein 8.2	Meilenstein für den Kontext **SAP R/3**.	

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

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2	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 8.2	Meilenstein für den Kontext **SAP R/3 Analyseberechtigungen Add-on**.	

Tabelle 29: Patches für SAP R/3 Berechtigungsobjekte

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32292	Mapping der Tabelle USOBHASH	Fügt ein Mapping und einen Synchronisationsschritt ein, um aus dem Zielsystem Daten der Tabelle USOBHASH einzulesen.	32292
VPR#32963_1	Mappingänderungen zur Abbildung zusätzlicher Berechtigungsobjekte (Teil 1)	Ändert verschiedene Mappings, um externe Services, TADIR-Services und RFC-Funktionsbausteine in SAP Funktionen abbilden zu können. Ersetzt den Patch VPR#32292. Teil 1: Löscht bestehende Mappings. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. Voraussetzung für Patch **Mappingänderungen zur Abbildung zusätzlicher Berechtigungsobjekte (Teil 2)**.	32963
VPR#32963_2	Mappingänderungen zur Abbildung zusätzlicher Berechtigungsobjekte (Teil 2)	Ändert verschiedene Mappings, um externe Services, TADIR-Services und RFC-Funktionsbausteine in SAP Funktionen abbilden zu können. Teil 2: Fügt neue Mappings ein. Dieser Patch wird während der Aktualisierung des One Identity	32963

Patch ID	Patch	Beschreibung	Fehler ID
		Manager automatisch angewendet. Abhängig von Patch **Mappingänderungen zur Abbildung zusätzlicher Berechtigungsobjekte (Teil 1)**.	
	Meilenstein 8.2	Meilenstein für den Kontext **SAP R/3**.	

Tabelle 30: Patches für SharePoint

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2	Meilenstein für den Kontext **SharePoint**.	

Tabelle 31: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31779	Konfiguration zum Anlegen und Löschen von Websitesammlungen und Websites	Erweitert die Synchronisationskonfiguration, um Websitesammlungen und Websites anlegen und löschen zu können.	31779
	Meilenstein 8.2	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#32564	Konfiguration der Anzahl paralleler Anfragen	Fügt die Variable **Max. Parallel Queries** ins Standardvariablenset ein.	32564
VPR#33884	Konfiguration des Verbindungsparameters `KeepAlive`	Fügt die Variable **HTTP KeepAlive** ins Standardvariablenset ein.	33884
VPR#33978	Neue Variable zum Einstellen einer Standardzeitzone	Fügt eine Variable ins Standardvariablenset und die Verbindungsparameter ein, um eine Standardzeitzone festlegen zu können. Dieser Patch wird während der	33978

Patch ID	Patch	Beschreibung	Fehler ID
		Aktualisierung des One Identity Manager automatisch angewendet.	
	Meilenstein 8.2	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
	Meilenstein 8.2	Meilenstein für den Kontext **Universal Cloud Interface**.	

Tabelle 34: Patches für Unix

Patch ID	Patch	Beschreibung	Fehler ID
VPR#Patch32500	Korrektur der Variable **Elevation password**	Kennzeichnet die Variable **Elevation password** als geheimen Wert.	32500
VPR#33249	Neue Variablen und Verbindungsparameter zur Authentifizierung mit dem privaten SSH-Schlüssel	Fügt Variablen und Verbindungsparameter zur Authentifizierung mit dem privaten SSH-Schlüssel ein.	33249
	Meilenstein 8.2	Meilenstein für den Kontext **Unix**.	

Tabelle 35: Patches für den One Identity Manager Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33728	Aktualisierung des One Identity Manager Schemas	Aktualisiert das One Identity Manager Schema, um die Generierung von Synchronisationsprojekten mit dem One Identity Manager Konnektor zu unterstützen.	33728
	Meilenstein 8.2	Meilenstein für den Kontext **Datenbank**.	

Tabelle 36: Patches für den CSV-Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2	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 Konfigurationsparameter **QER | Person | UseCentralPassword | PermanentStore** wurde gelöscht.
- Der Systembenutzer **viITShop** wurde gelöscht.

  Verwenden Sie die rollenbasierte Anmeldung über entsprechende Anwendungsrollen.
- Das Skript `VI_BuildPwdMessage` wurde gelöscht.

  Zum Versenden der E-Mail-Benachrichtigungen mit Anmeldeinformationen werden Mailvorlagen verwendet. Die Mailvorlagen sind in den Konfigurationsparametern **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** und **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** eingetragen.
- Die Sektion `<SpecialSheetData>` bei der Konfiguration von Oberflächenformularen wird nicht mehr unterstützt. Die Definition erfolgt jetzt über die Sektion `<Properties>`.
- Das Skript `UCI_TargetUsesProfiles` wurde gelöscht.

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

- Der generische LDAP Konnektor wird in zukünftigen Versionen nicht mehr unterstützt. Verwenden Sie den neuen LDAP Konnektor **LDAP Konnektor (Version 2)**.
- Der SOAP Web Service wird in zukünftigen Versionen nicht mehr unterstützt.
- Der SPML Webservice wird in zukünftigen Versionen nicht mehr unterstützt.
- Der Microsoft Exchange 2010 Konnektor wird in zukünftigen Versionen nicht mehr unterstützt.
- Der SharePoint 2010 Konnektor wird in zukünftigen Versionen nicht mehr unterstützt.
- 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
- TSB_CreateCanonicalNameFromDN
- VI_ConvertDNToCanonicalName
- VI_PersonAuto_LDAP
- VI_PersonAuto_ADS
- VI_PersonAuto_EBS
- VI_PersonAuto_Notes
- VI_PersonAuto_SAP
- VI_PersonAuto_SharePoint_SPSUser

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.

Minimalanforderungen für 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 2017 Standard Edition (64-Bit) mit aktuellem kumulativen Update • SQL Server 2019 Standard Edition (64-Bit) mit aktuellem kumulativen Update HINWEIS: Das kumulative Update 2 für SQL Server 2019 wird nicht unterstützt. HINWEIS: Aus Performancegründen wird für produktive Systeme der Einsatz der SQL Server Enterprise Edition empfohlen. • Kompatibilitätsgrad für Datenbanken: SQL Server 2017 (140) • 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 Produkt-Support.

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 4.7.2 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-	40 GB

tenspeicher	
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 4.7.2 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 4.7.2 oder höher
	• Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.7.2 und den Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions
	  • Web Server > Application Development > ISAPI Filters
	  • Web Server > Security > Basic Authentication
	  • Web Server > Security > Windows Authentication
	  • Web Server > Performance > Static Content Compression
	  • Web Server > Performance > Dynamic Content Compression
	Linux Betriebssysteme
	• NTP - Client
	• Mono 5.14 oder höher
	• Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
	  • mod_mono
	  • rewrite
	  • ssl (optional)

Minimalanforderungen für Anwendungsserver

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 4.7.2 oder höher
	• Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.7.2 und den Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions

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

Linux Betriebssysteme

- NTP - Client
- Mono 5.14 oder höher
- Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
  - mod_mono
  - rewrite
  - ssl (optional)

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 2010 ab Service Pack 3 • Microsoft Exchange 2013 mit kumulativem Update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 mit kumulativem Update 1 • MicrosoftExchange Hybrid-Umgebungen
SharePoint Konnektor	• SharePoint 2010 • SharePoint 2013 • SharePoint 2016 • SharePoint 2019
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

Konnektor	Unterstützte Datensysteme
	• HCL Notes Client Version 11.0.1 und 12.0
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 und 7.4.5
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) und RFC 7644 (System for Cross-domain Identity Management:

Konnektor	Unterstützte Datensysteme
	Protocol) sind zu gewährleisten.
Exchange Online Konnektor	• Microsoft Exchange Online
Google Workspace Konnektor	• Google Workspace
Oracle E-Business Suite Konnektor	• Oracle E-Business Suite System Version 12.1 und 12.2
SharePoint Online Konnektor	• Microsoft SharePoint Online
One Identity Safeguard Konnektor	• One Identity Safeguard Version 6.0, 6.7, 6.10 und 6.11

Produktlizenzierung

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

Upgrade und Installationsanweisungen

Um One Identity Manager 8.2 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 89.

Hinweise zur Aktualisierung des One Identity Manager

- 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 8.2 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 8.2 werden diverse Spalten zu physischen Pflichtfeldern, die bereits semantisch als Pflichtfelder definiert waren.

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

  ```
  <Tabelle>.<Spalte> must not be null

  Cannot insert the value NULL into column '<Spalte>', table '<Tabelle>';
  column does not allow nulls.

  UPDATE fails
  ```

  Prüfen und korrigieren Sie vor der Aktualisierung einer One Identity Manager-Datenbank die Daten. Im Add-on für das Konfigurationsmodul auf dem Installationsmedium wird ein Prüfskript bereitgestellt (`\SDK\SQLSamples\Files\MSSQL2K\30374.sql`). Im Fehlerfall korrigieren Sie die Daten und starten Sie die Aktualisierung erneut.
- One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe.
  Der Datenbankserver muss die extreme Transaktionsverarbeitung (XTP) unterstützen. Ist XTP nicht aktiviert, wird die Installation oder Aktualisierung nicht gestartet. Prüfen Sie, ob für den SQL Server die Eigenschaft **Extreme Transaktionsverarbeitung unterstützt** (Is XTPSupported) auf den Wert **True** gesetzt ist.

  Für die Erstellung speicheroptimierter Tabellen sind folgende Voraussetzungen zu erfüllen:

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

  Vor einer Installation oder Aktualisierung der One Identity Manager-Datenbank prüft der Configuration Wizard, ob diese Anforderungen erfüllt sind. Es werden im Configuration Wizard Reparaturmethoden angeboten, um die Datenbankdatei und die Datendateigruppe zu erstellen.
- Während der Aktualisierung 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 oder einer neuen One Identity Manager History Database mit der Version 8.2 sowie der Aktualisierung einer One Identity Manager-Datenbank oder One Identity Manager History Database von Version 8.0.x auf die Version 8.2 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 8.2 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 8.2

WICHTIG: Beachten Sie die Hinweise zur Aktualisierung des One Identity Manager auf Seite 89.

Um eine bestehende One Identity Manager Installation auf die Version 8.2 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**.
      - Um eine One Identity Manager History Database zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.
   c. Klicken Sie **Installieren**.

Der Installationsassistent wird gestartet.

d. Folgen Sie den Installationsanweisungen.

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

3. 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 **140** 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 8.2 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**.

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

c. Klicken Sie **Installieren**.

   Der Installationsassistent wird gestartet.

d. Folgen Sie den Installationsanweisungen.

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

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

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

Um Synchronisationsprojekte auf die Version 8.2 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 dem Datenbankserver und auf allen Synchronisationsservern gestartet sein.

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

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

   Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 96.

Um einen Anwendungsserver auf die Version 8.2 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 8.2 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 8.2 zu aktualisieren

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

Um das Web Portal für Betriebsunterstützung auf die Version 8.2 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 8.2 zu aktualisieren

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

Anwenden von Patches für Synchronisationsprojekte

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

Bevor Sie einen Patch anwenden

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

HINWEIS: Beim Aktualisieren bestehender Synchronisationsprojekte werden immer die Verbindungsparameter aus dem 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. 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 66
- Patches für Synchronisationsprojekte auf Seite 67

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 2021.0011.0019.0000 für alle Module und die Anwendungsversion 8.2 v82-139719 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.