One Identity Manager 9.2

Versionshinweise

29. September 2023, 10:43 Uhr

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 9.2 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 9.1.1 aufgeführt.
Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

One Identity Manager 9.2 ist ein Minor Release mit neuen Funktionen und verbessertem Verhalten. Siehe Neue Funktionen auf Seite 2 und Verbesserungen auf Seite 8.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 9.1.1 ist, lesen Sie auch die Versionshinweise der vorangegangenen Versionen. Die Versionshinweise sowie Versionshinweise zu zusätzlichen Modulen, die auf der One Identity Manager-Technologie basieren, finden Sie unter One Identity Manager Support.

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

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

Über One Identity Manager 9.2

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 dem One Identity Manager können Sie Access-Governance-Anforderungen in Ihrem gesamten Konzern plattformübergreifend verwirklichen. One Identity Manager basiert auf einer 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 https://www.cloud.oneidentity.com/.

Neue Funktionen

Neue Funktionen in One Identity Manager 9.2.

Allgemein

- Unterstützung von Amazon RDS for SQL Server als Datenbanksystem.
- Es wird eine Konfigurationsbibliothek mit Varianten für Bildungsregeln und für Formatierungsskripte bereitgestellt. Es werden verschiedene Bildungsregeln für die Spalten `CentralAccount`, `CentralEBSAccount`, `CentralSAPAccount`, `DefaultEmailAddress` und `InternalName` an Tabelle `Person` sowie verschiedene Formatierungsskripte mitgeliefert.
- Maschinelles Monitoring des Verarbeitungsstatus von Objektänderungen

  Nachdem Objekte im One Identity Manager geändert wurden, kann die Verarbeitung dieser Änderungen über eine Schnittstelle (REST API) maschinell überwacht werden. Die REST API gibt bei jeder Objektaktion die resultierende Prozess-ID zurück. Über diese Prozess-ID können verschiedene Informationen über die Prozesse, welche die Objektänderungen verarbeiten, abgeholt werden.

- Die Funktionalität der Prozessfunktion `FileComponent.ModifyFileAccess_DotNet` wurde erweitert.

  Ein neuer Parameter `AccessControlList` erlaubt die Konfiguration von mehreren Einträgen der Zugriffsberechtigungen. Die Prozessfunktion `ModifyFileAccess_Universal` wurde in Standardprozessen durch diese Prozessfunktion ersetzt.

  > WICHTIG: In den Prozessen zum Erzeugen der Homeverzeichnisse und Profilverzeichnisse für Active Directory Benutzerkonten werden die Konfigurationsparameter **QER | Person | User | AccessRights | HomeDir | EveryOne**, **QER | Person | User | AccessRights | ProfileDir | EveryOne**, **QER | Person | User | AccessRights | TerminalHomeDir | EveryOne** und **QER | Person | User | AccessRights | TerminalProfileDir | EveryOne** nicht mehr berücksichtigt.
  >
  > Stellen Sie sicher, dass in den Basisverzeichnissen, beispielsweise dem Homeverzeichnis, keine Berechtigungen für die Benutzergruppe Jeder (`EveryOne`) an die untergeordneten Verzeichnisse vererbt werden. Andernfalls besteht die Möglichkeit, dass die Benutzergruppe ungewollte Berechtigungen auf alle Home-Verzeichnisse erhält.

HTML-Webanwendungen

> HINWEIS: Neue Funktionen für das Web Portal wurden für die HTML-Anwendung implementiert, nicht für das Web Designer Web Portal.

- Im Web Portal wird eine kontextsensitive Hilfe angeboten. Es werden Hilfetexte und Links zu den Anwenderhandbüchern angezeigt.
- Im Web Portal werden nun für bestimmte Eigenschaften Beschreibungstexte als Hilfe angezeigt.
- Im Web Portal kann man nun Identitäten und deren Eigenschaften miteinander vergleichen.
- Man kann nun im Web Portal die Verantwortlichkeiten der Identitäten anzeigen, für die man verantwortlich ist. Zusätzlich kann man die angezeigten Identitäten auf Identitäten einschränken, die das Unternehmen verlassen haben oder bald verlassen werden.
- Um die für ein Team erforderlichen Berechtigungen auf einfache Weise pflegen zu können, kann man nun eine Rolle für die Identitäten erstellen, für die man verantwortlich ist.
- **TECH PREVIEW ONLY**: Das Web Portal unterstützt die Bearbeitung von Entscheidungsworkflows.

  > HINWEIS: Diese Funktion ist nur für Benutzer verfügbar, die über die Programmfunktion **Portal_Preview_WorkflowEditor** verfügen.
- Im Web Portal kann man nun für offene Bestellungen eine Entscheidungshilfe anzeigen.
- Im Web Portal können nun archivierte Bestellungen angezeigt werden.

- Im Web Portal kann man nun für offene Attestierungsvorgänge eine Entscheidungshilfe anzeigen.
- Im Web Portal kann man nun Richtlinienverbunde bearbeiten.
- Im Web Portal steht nun eine Funktion zur Verfügung, die Empfehlungen für die Zuweisung von Berechtigungen an Abteilungen, Anwendungsrollen, Geschäftsrollen, Kostenstellen, Standorten oder Systemrollen gibt.
- Der Verantwortliche einer Software-Anwendung sieht nun im Web Portal die Identitäten, die Zugriff auf die Software-Anwendung haben.
- Im Web Portal kann man nun benutzerdefinierte Designs einbinden und verwenden.
- Im Web Portal kann man nun Übersetzungen für Namen und Beschreibung von Anwendungen pflegen.
- Im Web Portal kann man nun Suchbegriffe als Filter verwenden. Dazu muss man den gewünschten Begriff in das Suchfeld eingeben und anschließend die **Enter**-Taste drücken.
- Im Web Portal für Betriebsunterstützung kann man nun die Inhalte der DBQueue anzeigen.
- Im Web Portal für Betriebsunterstützung werden nun ausstehende Objekte nur für Zielsysteme angezeigt, für die der Benutzer verantwortlich ist.
- Im Web Portal für Betriebsunterstützung sieht man nun die abgeschlossenen oder noch offenen Operationen im System, die zu einer konkreten Prozess-ID gehören.
- Im Web Portal für Betriebsunterstützung kann man nun eine Operationshistorie anzeigen. Die Operationen können nach Zeitpunkt, Änderungsart und auslösenden Nutzer gefiltert werden.
- Im Web Portal für Betriebsunterstützung kann man nun die Prozesshistorie anzeigen.
- Im Administrationsportal können nun Protokolldateien eingesehen und heruntergeladen werden.

Zielsystemanbindung

- An Property-Mapping-Regeln kann konfiguriert werden, ob beim Erkennen unzulässiger Änderungen die Reihenfolge der Werte von mehrwertigen Schemaeigenschaften beachtet werden soll.
- Erweiterung des RemoteConnectPlugin

  Das RemoteConnectPlugin wurde erweitert. Zum Herstellen einer Remoteverbindung zum Zielsystem können weitere Authentifizierungsverfahren genutzt werden. Zusätzliche Eigenschaften, wie Timeout oder Zertifikate, können konfiguriert werden.
- Wenn im Synchronization Editor Systemfilter oder Objektfilter erstellt werden, kann getestet werden, ob die Filterbedingung die korrekten Ergebnisse liefert.
- Änderungen an virtuellen Schemaeigenschaften können direkt im Mappingeditor des Synchronization Editor getestet werden.

- Die rollenbasierte Zugriffssteuerung (RBAC) und das Priviliged Identity Management (PIM) für Azure Active Directory werden im neuen "RBAC" und "PIM" Modus unterstützt. Aufgrund von Einschränkungen der Microsoft Graph API unterstützt die Rollenmanagement Funktion im One Identity Manager im Modus "PIM" ausschließlich den globalen Verzeichnisbereich für aktive Rollenzuweisungen. Eine manuelle Aktivierung der Funktionen ist erforderlich.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35513 bereitgestellt.
- Für Azure Active Directory Benutzerkonten werden zusätzliche Identity Management-relevante Schemaeigenschaften abgebildet.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36729 bereitgestellt.
- Es werden zusätzliche Schemaeigenschaften für den letzten Anmeldezeitpunkt von Azure Active Directory Benutzerkonten abgebildet. Auf diese Schemaeigenschaften kann nur zugegriffen werden, wenn eine Azure Active Directory-Premium-Lizenz vorhanden ist.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#33776 bereitgestellt.
- Hierarchische Adressbücher aus Exchange Online werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35780 bereitgestellt.
- Microsoft Teams Teamvorlagen werden unterstützt.
- POSIX-Erweiterungen für Active Directory Benutzerkonten, Gruppen und Kontakte werden unterstützt.

  Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#14634 und VPR#14634_ARS bereitgestellt.
- Hierarchische Adressbücher aus Microsoft Exchange werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35779 bereitgestellt.
- Active Roles Version 8.1.3 wird im bisherigen Umfang unterstützt.
- One Identity Manager unterstützt die LDAP-Objektklasse **eduPerson**. Diese Objektklasse wird vorrangig in Verzeichnissen von Universitäten und Hochschulen verwendet, um die Kommunikation zwischen den Einrichtungen zu erleichtern.
- One Identity Safeguard Versionen 7.2 und 7.3 werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36617 bereitgestellt.
- One Identity Safeguard Partitionen werden unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36044 bereitgestellt.

- SAP .Net Connector 3.1 for x64, mindestens Version 3.1.2.0, für Microsoft .NET 4.8 wird unterstützt.
- Das Roaming von Notes Benutzerkonten wird unterstützt.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36087 bereitgestellt.
- Der SCIM Konnektor unterstützt die Synchronisation von SAP Cloud ALM Anwendungen über SAP Cloud Identity Services mit dem Standardschema. Zum Einrichten der Synchronisation kann die Projektvorlage **SCIM Synchronisation einer SAP Cloud ALM Anwendung** genutzt werden.
- Information über die letzte Kennwortänderung und das letzte Anmeldedatum von Unix Benutzerkonten werden abgebildet.

  Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36688 bereitgestellt.

Identity Management und Access Governance

- Umbenennungen

  In diesem Zusammenhang wurden ungenutzte Übersetzungen in der Tabelle `DialogMultiLanguage` aufgeräumt.

  - **Personen** und **Mitarbeiter** zu **Identitäten**

    One Identity Manager verwaltet nicht nur natürliche Personen, sondern verschiedenste Identitätstypen. Zur Verdeutlichung wurden die Benennungen **Person** und **Mitarbeiter** für den Objekttyp `Person` in **Identität** umbenannt. In diesem Zusammenhang wurde **Pseudo-Person** in **Virtuelle Identität** umbenannt.
  - **Bestellvorlagen** zu **Produktpakete**
  - **Helpdesk-Calls** zu **Tickets**
  - **Sprachkultur** zu **Sprache** oder **Sprachcode**
- Behavior Driven Governance für One Identity Safeguard wird unterstützt. Dazu gehören:
  - Attestierung und Rezertifizierung der Mitgliedschaften in PAM Benutzergruppen für Benutzerkonten, die innerhalb eines definierten Zeitraums keine Zugriffsanforderungen gestellt haben. Nach abgelehnter Attestierung werden die Mitgliedschaften automatisch entfernt. Der Zeitraum wird über den Konfigurationsparameter **TargetSystem | PAG | UnusedThresholdInDays** eingestellt.
  - Ermittlung von PAM Berechtigungen, wie Assets, Benutzergruppen oder Nutzungsrechte, die für einen definierten Zeitraum nicht genutzt wurden. Wenn eine Berechtigung laut PAM Prüfprotokoll in diesem Zeitraum nicht genutzt wurde, kann in einem Rezertifizierungsverfahren entschieden werden, ob die Berechtigung weiterhin benötigt wird. Ungenutzte Berechtigungen können anschließend im Zielsystem entfernt werden. Der Zeitraum wird über

den Konfigurationsparameter **TargetSystem | PAG | UnusedThresholdInDays** eingestellt.

- Neues Entscheidungsverfahren **OX - Eigentümer des Objekts in beliebigem Parameter der Bestelleigenschaften**

  Das Entscheidungsverfahren ermittelt als Entscheider den Eigentümer (Anwendungsrolle) eines Objekts, das in einem Bestellparameter angegeben ist. Die Anwendungsrolle ist dem Objekt über eine Fremdschlüsselspalte zugeordnet. Am Entscheidungsschritt wird der Name des Bestellparameters angegeben, sowie der Name der Tabellenspalte, welche auf die Anwendungsrolle verweist. Das Entscheidungsverfahren kann für alle Produkte genutzt werden, denen eine Bestelleigenschaft zugeordnet ist, die diesen Bestellparameter verwendet.
- An Attestierungsrichtlinien können Nutzungsbedingungen zugeordnet werden. Die Nutzungsbedingungen können als PDF-Datei in verschiedenen Sprachen bereitgestellt werden.
- Im Web Portal können Attestierern Entscheidungsempfehlungen gegeben werden. Die Empfehlungen zur Genehmigung oder Ablehnung von Attestierungsvorgängen werden anhand verschiedener Kriterien berechnet. Die Kriterien werden an den Konfigurationsparametern unterhalb von **QER | Attestation | Recommendation** spezifiziert.

  HINWEIS: Die Funktion wurde für das Web Portal HTML-Anwendung implementiert, nicht für das Web Designer Web Portal.
- An Attestierungsvorgänge können jetzt Zusatzeigenschaften zugewiesen werden.
- An Attestierungsrichtlinien kann konfiguriert werden, ob ein leerer Attestierungslauf generiert werden soll, wenn bei der Berechnung der Attestierungsvorgänge kein zu attestierendes Objekt ermittelt wird.
- Neue Entscheidungsverfahren **BA - Eigentümer der Anwendung** und **BE - Entscheider der Anwendungsberechtigung**

  Die Entscheidungsverfahren ermitteln die Eigentümer (Anwendungsrolle) beziehungsweise Entscheider (Anwendungsrolle) der zugehörigen Anwendung bei der Attestierung von Anwendungsberechtigungen im Application Governance Modul.
- Neues Entscheidungsverfahren **SP - Eigentümer des Dienstprinzipals**

  Das Entscheidungsverfahren ermittelt die Eigentümer (Anwendungsrolle) des attestierten Azure Active Directory Dienstprinzipals.

Siehe auch:

- Verbesserungen auf Seite 8
- Gelöste Probleme auf Seite 31
- Schemaänderungen auf Seite 54
- Patches für Synchronisationsprojekte auf Seite 63

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die in One Identity Manager 9.2 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Das Update-Ereignis wird nur generiert, wenn das Objekt Änderungen hatte.	30163
Die Unit of Work verhindert, dass Objektänderungen nach dem Start des Commits hinzugefügt werden, da diese sonst verloren gehen würden.	35913
Einführung einer Bulk-Query-Schnittstelle in der VI.DB, die besonders Frontends beschleunigen kann.	36478
Im Konsistenzeditor können die Konsistenzprüfungen für die Testeinstellungen gefiltert werden.	32390
Verbesserte Konsistenzprüfung **DialogDeferredOperation with overdue actions, activated but without existing job**.	34789
Die Konsistenzprüfung auf Verwendung des SQL-Formatters prüft nun auch die richtige Parametrisierung der `EmptyClause` für Schlüsselspalten.	35737
Der Konsistenztest **Objectkey references to non existing object (tolerated)** wird nicht mehr benötigt und wurde entfernt.	37141
Performanceverbesserung sowie verbesserte Handhabung der Syntaxvervollständigung bei der Eingabe von Skriptcode.	35649
Die Funktionsauswahl zum Skriptaufruf im Skripteditor im Designer wurde verbessert. Es wird versucht, das jeweils ausgewählte Skript vorauszuwählen.	36081
Verbesserte Darstellung der Erweiterungen für Proxyviews im Schemaeditor im Designer.	36380
Verbesserungen der Benutzeroberfläche zur Unterstützung von Änderungen an mehrsprachig übersetzten Daten.	34794
Die automatische Übersetzung von zusammengesetzten Zeichenketten wird unterstützt. Es werden die Übersetzungen der einzelnen Bestandteile ermittelt und zum kompletten Inhalt zusammengesetzt.	34477
Im Wörterbucheditor im Designer werden kundenspezifische Änderungen an Standardübersetzungen in der Übersetzungstabelle gelb hinterlegt.	36422
Das Format für die Konfigurationsdaten der Formulardefinition wurde überarbeitet. Kundenspezifische Formulardefinitionen werden automatisch konvertiert.	35422

Verbesserung	Fehler ID
Die Informationen in Spalte `DialogLogicalForm.DialogFormDefinition` werden beim Speichern jetzt aus eine gültige XML-Notation überprüft.	36125
Die Maskierung von Freitext-Variablen in der Navigation der Benutzeroberfläche wurde verbessert. Der Anwender kann bei der Verwendung nun Einfluss auf die Maskierung von Sonderzeichen nehmen.	35886
Mit einem Skript können Variablen der Benutzeroberfläche dynamisch und kontextabhängig berechnet werden. Damit können Anzeigetexten in der Benutzeroberfläche kontextabhängig gestaltet werden.	36305, 36238, 36862
Implementierung eines Skriptes zur Sichtbarkeit an diversen Standardmethoden. Somit werden diese Methoden im Aufgabenmenü des Managers nicht mehr angezeigt, wenn sie aufgrund einer objektspezifischen Bedingung nicht ausführbar wären.	36509
Im Manager wird für diverse Zuweisungsformulare eine Beschreibung als Tooltipp eingeblendet.	32033
Ein neues Steuerelement ermöglicht das komfortable Pflegen von komplexen Datenstrukturen, welche datenbankseitig beispielsweise im Json Format oder auch im .NET Datenbank-ConnectionString- Format gespeichert werden.	35518
Verbesserte Barrierefreiheit des Steuerelementes für hierarchische Listen.	36640
Der Ablehnungsgrund für Sitzungszertifikate im Anwendungsserver wird jetzt per NLog protokolliert.	35618
Im Anwendungsserver wird nun auf der Kachel mit den Systeminformationen die Produktversion angezeigt.	35963
Das Programm `AppServer.Installer.CMD.exe` wird nun analog zu den anderen Kommandozeilenprogrammen lokal installiert.	35894
Es ist nun mithilfe des Web Installers möglich, eine bestehende Anwendungsserver-Installation zu bearbeiten.	33584, 314733
In der Protokolldarstellung des One Identity Manager Service wird über das Menü **Raw Log** das NLog-Protokoll inklusive der Einträge von Plugins angezeigt.	35763
Die für den Database Agent Service nicht mehr notwendigen Berechtigungen auf der Systemdatenbank **msdb** wurden entfernt.	35337
Das Programm `DatabaseAgentServiceCmd.exe` schreibt nun alle Warnungen und Fehler in die Konsolenausgabe.	36134
Im E-Mail-Konfigurationsassistenten kann jetzt ein Jobserver festgelegt werden, der die Funktion **SMTP-Server** übernimmt.	35564
Bei der Generierung von Prozessen für E-Mail-Benachrichtigungen werden	33690

Verbesserung	Fehler ID
Fehlermeldungen protokolliert, wenn die entsprechenden Konfigurationsparameter nicht aktiviert sind oder keine gültige E-Mail-Adresse eingetragen ist.	
Im Job Queue Info werden deaktivierte Jobserver nun besser dargestellt.	35677
Im Job Queue Info wurde das Verhalten das Stoppen und Starten des Systems (Not-Aus) verändert, um im Notfall die Abarbeitung der Queues möglichst verzögerungsfrei zu stoppen.	36222
Verbesserte Darstellung der Fehlermeldung von Prozessschritten im Job Queue Info. Ein Dialog mit der vollständigen Fehlermeldung kann über den Fehlerlink oder auch das Kontextmenü geöffnet werden.	36918
Die Anordnung der Schaltfläche für den Not-Aus in der Symbolleiste des Job Queue Info wurde verbessert.	37105
Die Protokollierung in Datenbanken mit NLog 5 ist nun möglich.	36303
Tritt beim Speichern ein Fehler auf, werden nun sowohl der Tabellenname als auch der Anzeigename des Objektes ausgegeben, um das fehlerhafte Objekt besser lokalisieren zu können.	36373
Verbesserter Ausgabe von Fehlermeldungen aus der Datenbank.	36639
Die automatische Textvervollständigung im Filter Object Browser wurde verbessert.	36083
Der Leerraum in der Filteransicht des Object Browser wurde entfernt.	36084
Performanceverbesserung beim Import kumulativer Transporte mit dem Database Transporter.	36401
Verbesserungen im Kommandozeilenprogramm `DBTransporterCMD.exe`.	37012, 37013
Diverse Verbesserungen in der Benutzeroberfläche des Programms Data Import.	36611
Der Software Loader zeigt eine Warnmeldung, wenn die gewählten Dateien für den Import nicht in einem gültigen Installationsverzeichnis liegen.	35609
Die horizontale Leseskalierung in lokalen Verfügbarkeitsgruppen eines SQL Server Clusters werden nun besser unterstützt. • In die Konfigurationsdateien der Anwendungen wurden Vorlagen zur Konfiguration für die horizontale Leseskalierung integriert. • Die verschiedenen Verbindungspools sind nun im Protokoll ersichtlich.	36109, 36110, 36977, 37029
Performanceverbesserung beim Aufräumen des Puffers für DBQueue Prozessor-Aufträge.	35978

Verbesserung	Fehler ID
Es erfolgt nun keine Prozessauslieferung, wenn es kundenspezifische Datenbanktrigger gibt, die deaktiviert sind.	36433
Columnstore-Indizes werden beim Erstellen eines Transports mit dem Database Transporter ausgeschlossen.	36452
Nicht-benötigte Berechtigungen auf die Tabelle `PersonPasswordHistory` wurden entfernt.	36940, 419127
Performanceverbesserung beim Befüllen der Tabelle `QBMSplittedLookup`.	36973
Die Index-Wichtung für die Volltextsuche kann nun auch für Integer-Spalten gesetzt werden.	36801
Für die Dauer der Komprimierung der DBQueue werden keine Trigger mehr deaktiviert. Damit schaltet die Datenbank nicht in den Wartungsmodus und die Anwender werden nicht beeinträchtigt.	36975
Für eine HTML-Anwendung kann ein Datenbankbenutzer angegeben werden, dessen Berechtigungsebene mindestens benötigt wird, um diese HTML-Anwendung verwenden zu können.	36436
Performanceverbesserung Sichtbarkeitsbedingungen für verschiedene Anwendungsrollen.	36759
Nach einer Datenbankmigration werden die Daten für die Moduldefinition des Kundenmoduls **CCC** neu generiert.	36820
Überflüssige Rollendefinitionen für die History Database wurden entfernt. Es wird ein SDK-Skript für das Anlegen der minimal erforderlichen Berechtigungen bereitgestellt.	35936
Im Schema Extension können kundenspezifische Spalten in View-Tabellen gelöscht werden.	36667
Bei entsprechender Konfiguration, kann ein Bericht beim Klick auf den Bericht sofort in ein vorgegebenes Format exportiert werden.	35607
Die Einstellungen zur Abfrage und zur Berechnung für Berichtsparameter können über das Skript für Datenabhängigkeiten geändert werden, das Frontend passt sich automatisch an.	36573
Where-Klauseln aus der Berichtsdefinition von abonnierbaren Berichten werden nun ebenfalls als vertrauenswürdig markiert.	36574
Durch die neuen Kommandozeilenparameter `/Conn` und `/Auth` am System Debugger kann die Anmeldeinformationen direkt übergeben werden und damit eine automatische Anmeldung erfolgen.	36403
Mit dem Programm `Quantum.MigratorCmd.exe` können nun kundenspezifische Berechtigungsgruppen erstellt werden (Parameter `/Group`) sowie SQL-Anweisungen nach der Datenbankinstallation	35746

Verbesserung	Fehler ID
ausgeführt werden (Parameter `/PostSQL`).	
Im Installationsassistenten werden auf der Seite **Modulauswahl** zusätzliche Beschreibungen zu den einzelnen Modulen angezeigt, wenn man sie auswählt.	35830
Für die Nutzung des RemoteConnectPlugins in Docker-Containern wurde ein neues Autorisierungsverfahren implementiert.	36454
Aktualisierung von Drittanbieterkomponenten.	36426
Die Sicherheit beim Generieren von Berichten wurde erhöht.	37255

Tabelle 2: HTML-Webanwendungen: Herstellen der Funktionsgleichheit zum Web Designer Web Portal

Verbesserung	Fehler ID
Es ist im Web Portal nun möglich, die derzeitige Ansicht einer Seite zu speichern.	32356, 30242, 300743
Im Web Portal kann man nun, abhängig von den Berechtigungen des angemeldeten Benutzers, Statistiken und KPIs anzeigen.	36789, 393878, 322309
Im Web Portal wurde der Filterdialog überarbeitet und eine Möglichkeit hinzugefügt, benutzerdefinierte Filter zu erstellen.	206836
Im Web Portal kann man nun anderen Identitäten Anfragen zu Bestellungen senden.	250607
Im Web Portal kann man nun in der Historie eines Objekts eine Zustands-übersicht und einen Zustandsvergleich anzeigen.	252817
Im Web Portal kann man nun Webauthn-Sicherheitsschlüssel verwalten, sofern der API Server zusammen mit RSTS konfiguriert ist.	259005
Im Kennwortrücksetzungsportal kann man nun Kennwortfragen verwalten.	277546
Im Web Portal kann man nun in Tabellen sortieren.	284241
Im Web Portal kann man nun Ressourcen, Zuweisungsressourcen, mehrfach bestellbare Ressourcen und mehrfach zu-/ abbestellbare Ressourcen verwalten.	288423
Im Web Portal ist es nun möglich, Abteilungen, Anwendungsrollen, Geschäftsrollen, Kostenstellen, Standorte und Systemrollen zu erstellen.	288860
Manager, IT Shop Administratoren und Compliance & Security Officer können Bestellungen von Identitäten einsehen.	290759
Im Web Portal kann man nun die Historie von Systemberechtigungen	299095

Verbesserung	Fehler ID
anzeigen.	
Im Web Portal kann man nun Inhalte von Tabellen exportieren.	300508
Im Web Portal kann man nun Tickets anzeigen, erstellen und bearbeiten.	304631, 305721
Im Web Portal kann man nun die Stammdaten von Risikoberechnungsvorschriften bearbeiten.	304675
Im Web Portal kann man nun mithilfe der Funktionsanalyse Identitäten mit kritischen SAP-Funktionen anzeigen, die Complianceregeln verletzen. Zusätzlich kann man mithilfe der Regelanalyse Complianceregeln anzeigen, die SAP-Funktionen beinhalten, und jede Identität identifizieren, die die Complianceregeln verletzt.	304676
Die Verwaltung von Regelverletzungen im Web Portal wurde erweitert: • Es werden mehr Details zu Regelverletzungen angezeigt. • Risikomindernde Maßnahmen, die einer Regelverletzung zugewiesen sind, werden angezeigt. • Die Ermittlung von Regelverletzungen kann manuell gestartet werden.	305793
Im Web Portal kann man nun nach Attestierungsvorgängen filtern, in denen eine bestimmte Identität eine Entscheidung getroffen hat.	305996
Im Web Portal können Auditoren nun Identitäten anzeigen.	306003
Im Web Portal können Auditoren nun Abteilungen, Anwendungsrollen, Geschäftsrollen, Kostenstellen, Standort und Systemrollen anzeigen.	306005
Im Web Portal kann man nun Unternehmensrichtlinien anzeigen.	306100
Im Web Portal können Compliance-Framework-Verantwortliche und Auditoren nun Complianceregeln anzeigen.	308021
Im Web Portal erfordert die Zustimmung zu den Nutzungsbedingungen nun eine explizite erneute Authentifizierung des angemeldeten Benutzers. Das Authentifizierungsverfahren dafür ist konfigurierbar und kann deaktiviert werden.	314572
Das Web Portal unterstützt nun Browser-Benachrichtigungen.	319194
Im Web Portal kann man nun Bestellanfragen anzeigen und beantworten.	321526
Im Web Portal kann man nun Anfragen zu Attestierungsvorgängen an andere Identitäten senden.	321541
Im Web Portal kann man nun Anfragen zu Attestierungsvorgängen anzeigen und beantworten.	321542

Verbesserung	Fehler ID
Der Verantwortliche einer Software-Anwendung kann nun die Stammdaten der Software-Anwendung im Web Portal bearbeiten.	394940
Auditoren sehen nun im Web Portal alle Bestellungen.	400433
Im Web Portal kann man nun Listenberichte direkt im Browser darstellen.	405305
Im Web Portal kann man nun Geräte anzeigen und deren Stammdaten bearbeiten.	405829, 275567
Im Web Portal kann nun in der Bestellhistorie eine Bestellung erneut abgesendet werden.	413040
Das Web Portal zeigt Informationen zum angemeldeten Benutzer, dessen Berechtigungsgruppen und Programmfunktionen.	415628
Das Web Portal zeigt die Quelldaten zu bestimmten Statistiken an.	416009
Im Web Portal kann man nun für Unternehmensrichtlinien die zugehörigen Richtlinienverletzungen anzeigen.	416128
Im Web Portal können Manager nun Einzeldelegierungen und Stellvertretungen für Identitäten erstellen, für die sie verantwortlich sind.	420543
Im Web Portal sieht man nun die risikomindernden Maßnahmen, die an Unternehmensrichtlinien beziehungsweise Richtlinienverletzungen zugewiesen sind. Im Falle von Richtlinienverletzungen kann man die Zuordnungen der risikomindernden Maßnahmen auch bearbeiten.	421474
Im Web Portal kann man nun in den Profil-Einstellungen ein Hyperview für die angemeldete Identität anzeigen.	421695
Im Web Portal kann man nun für Attestierungsvorgänge und Richtlinienverletzungen Hyperviews für die beteiligten Objekte anzeigen.	425269

Tabelle 3: HTML-Webanwendungen

Verbesserung	Fehler ID
Es ist nun mithilfe des Web Installers möglich, eine bestehende API Server-Installation zu bearbeiten.	33584, 314733, 313398
Bei der Installation des API Server ist es möglich, das Kennwort des Standard-Systembenutzers **IdentityRegistration** zu setzen. Es ist ebenso möglich, einen anderen Systembenutzer anzugeben, unter dessen Anmeldung neue Identitäten angelegt werden.	36343, 407727
Der API Server kann in Protokolleinträgen die Sitzungs-ID mit ausgeben. In der Datei `nlog.config` muss im Abschnitt `<nlog>` dafür Folgendes eingetragen werden: `<extensions>`	36902

Verbesserung	Fehler ID
`<add assembly="QBM.CompositionApi.Server" />` `</extensions>`	

Lokale Anpassungen der Konfiguration eines API Server werden standardmäßig nur noch erlaubt, wenn der API Server über die Kommandozeile am `ImxClient` gestartet wurde.
Auf IIS-basierten Installationen sind lokale Anpassungen deaktiviert. Dieses Verhalten können Sie durch Hinzufügen des folgenden Code-Schnipsels in der Datei `web.config` übersteuern.
`<appSettings>`
`<add key="IsStandAlone" value="true" />`
`</appSettings>`
	416938

Der API Server unterstützt die Erstellung von Websocket-API-Methoden.	394642
Verbesserungen an den API Clients für Angular-Entwickler: • Für Parameter-Typen werden nun benannte Schnittstellen verwendet. Diese Schnittstellen werden exportiert, sodass sie im Anwendungscode verwendet werden können. • Die Eigenschaften der Parameter werden mit ihren Beschreibungstexten im API Client hinterlegt.	394386
Der API Server verwendet den HTTP-Statuscode 403 bei einer fehlgeschlagenen Authentifizierung.	405643
Der CSRF-Schutzmechanismus der SCIM-API des API Servers ist nun standardmäßig deaktiviert.	405926
Die API Clients sind stabiler gegenüber abgebrochenen Netzwerkverbindungen.	264940
Der API Server führt eine Versionsprüfung durch. Ein Zugriff durch API Clients anderer Versionen führt zu einer Fehlermeldung.	296243
Die Performance beim Start des API Servers wurde verbessert.	312481
Die Kompatibilität des API Servers mit Reverse-Proxies wurde verbessert. Im Administrationsportal können Reverse-Proxies konfiguriert werden.	319175
Der API Server belegt nun auf einer IIS-Installation weniger Speicherplatz für temporäre Dateien.	328741
Für die Bearbeitung eigener API-Plugins werden nun typsichere Klassen unterstützt.	316845
Der API Server beachtet nun alle Sprachen, die im Header `Accept-Languages` einer API-Anfrage aufgelistet werden.	316933

Verbesserung	Fehler ID
Für den API Server wurde die Extension-Methode `.WithSingleEntityRead()` implementiert, mit deren Hilfe man einzelne Entities über die API laden kann (identifiziert über den Primärschlüssel).	251366
Wenn die Basis-URL des API Servers keiner Webanwendung entspricht wird nun ein entsprechender Protokolleintrag generiert.	389277
Das Debugging von Angular-Anwendungen wurde durch die Verwendung der `deleteDestPath`-Option stabilisiert.	407356
Die Methoden der API Clients unterstützen nun den Abbruch von API-Anfragen.	390096
Im Administrationsportal wurde die Benennung mehrerer Konfigurationsschlüssel verbessert.	424491
Im Administrationsportal können nun neu hinzugefügte Konfigurationsschlüssel gelöscht werden.	307180
Die API-Dokumentation wird nun im Administrationsportal angezeigt. Zusätzlich kann die Anzeige der API-Dokumentation über die Konfiguration im Administrationsportal konfiguriert werden.	322436
Die Performance der API-Dokumentation wurde verbessert.	307709
Anfragen aus der API-Dokumentation (Swagger) schlagen nun nicht mehr aufgrund des fehlenden X-XSRF-TOKEN-Header fehl, da dieser nun in den Anfragen enthalten ist.	394255
Im Administrationsportal kann nun die SameSite-Cookie-Einstellung bearbeitet werden.	386427
Im Administrationsportal kann nun die Domain der vom API Server gesendeten Cookies konfiguriert werden.	388463
Im Administrationsportal kann nun ein Standard-Design für Webanwendungen konfiguriert werden.	322421
Die Webanwendungen unterstützen nun ein kontrastreiches Design.	316555
Im Administrationsportal wurden die wirkungslosen Konfigurationsparameter `VI_ITShop_CanCloneCartItemsByPerson` und `VI_ITShop_CanCloneCartItemsByProduct` entfernt.	422641
Im Administrationsportal wurde die Anzeige des API Server-Status verbessert: • Man kann die Liste der Composition-API-Caches anzeigen. • Man kann die Caches leeren. • Man kann die Verwendung der Caches aktivieren und deaktivieren. • Man kann auf der Startseite Diagramme anzeigen, die im zeitlichen	387864

Verbesserung	Fehler ID
Verlauf die Anzahl der Sessions anzeigen.	
Man kann nun im Administrationsportal konfigurieren, dass Benutzer die Sprache in ihren Profil-Einstellungen nicht ändern können und stattdessen die Browser-Sprache für die Oberflächen der Webanwendungen verwendet wird.	35813, 206640
Im Administrationsportal kann man nun die maximale Größe für das Profilbild einer Identität konfigurieren.	367838
Das Programm `ConfigFileEditorCMD` unterstützt nun den Kommandozeilen-Parameter `/preventdbupdate true`. Ist dieser gesetzt, findet keine Aktualisierung des Anwendungstokens in der Datenbank statt. Dieser Parameter ist primär für die Verwendung in Containern gedacht.	405743
Das Web Portal verwendet für die Suche nach Produkten auf der Produktauswahlseite einen neuen Modus, um vollständigere Suchergebnisse zu erhalten und die Performance zu erhöhen.	32800, 423711
Beim Entscheiden über eine Bestellung beziehungsweise einen Attestierungsvorgang wird nun angezeigt, in welchem Entscheidungsschritt man gerade entscheidet.	34861, 316872
Man kann nun für Produkte, die einem Produktpaket zugewiesen sind, Werte für Bestellparameter angeben. Diese Werte werden dann beim Bestellen aus dem entsprechenden Produktpaket vorausgefüllt.	33637, 316846
Der Anwender erhält nun vor dem Speichern und vor dem Starten einer Attestierungsrichtlinie eine Warnung, falls die erwartete Anzahl der Attestierungsvorgänge einen bestimmten Schwellwert überschreitet. Der Schwellwert ist konfigurierbar.	34918, 305302
Die Seite **Neue Bestellung** des Web Portals wurde komplett überarbeitet.	35573, 312077
Performanceverbesserungen im Web Portal: • beim Genehmigen von Attestierungsvorgängen • beim Anzeigen meiner Verantwortlichkeiten	35861, 36814
Es werden neue Attestierungsbedingungen zur Identifikation ungenutzter Benutzerkonten angeboten, die für die Attestierung von Benutzerkonten und Mitgliedschaften in Systemberechtigungen genutzt werden können.	37004
Es werden neue Attestierungsbedingungen zur Identifikation ungenutzter PAM Berechtigungen angeboten, die beispielsweise im Rahmen des Behavior Driven Governance für One Identity Safeguard genutzt werden können.	37005, 37006
Im Web Portal wurde die Bedienbarkeit per Tastatur verbessert.	410172

Verbesserung	Fehler ID
IT Shop-Administratoren können nun im Web Portal Produktpakete bearbeiten.	416274
Im Web Portal kann man nun eine neue Systemrolle für eine Anwendung erstellen, ohne dieser Systemrolle gleichzeitig Berechtigungen zuzuweisen.	421193
Im Web Portal können nun Anwendungsberechtigungen einer Anwendung gefiltert werden.	425214
Verbesserungen beim Bearbeiten von Leistungspositionen: • Im Web Portal sieht man, welcher Anwendung die Anwendungsberechtigung einer Leistungsposition zugewiesen ist. • Falls Eigenschaften einer Leistungsposition durch die Zuweisung zu einer Anwendungsberechtigung nicht bearbeitbar sind, wird ein entsprechender Hinweis angezeigt. • IT Shop Administratoren können den Eigentümer einer Leistungsposition ändern.	292570
Wenn Complianceregeln für SAP Funktionen verletzt werden, kann man nun im Web Portal die SAP Berechtigungen anzeigen, welche zur Regelverletzung führen.	297236
Im Web Portal kann man nun bestimmte Eigenschaften für mehrere Produkte, die man bestellen möchte, auf einmal festlegen (beispielsweise Gültigkeit und Begründungen).	309614
Als Berichtsadministrator kann man nun im Web Portal festlegen, wer einen Bericht aufrufen beziehungsweise abonnieren kann.	314124
Im Web Portal kann man nun persönliche Einstellungen vornehmen: • Design der Anwendung • Zeitzone • Verwendung der Profilsprache statt der Browser-Sprache	319031, 206656
Für das Web Portal können nun für mehrere Seiten die Ansichten konfiguriert werden: • Attestierungsläufe • Regelverletzungen • Identitäten-Übersicht im Daten-Explorer • Systemberechtigungsübersicht im Daten-Explorer	320784
Beim Bestellen aus einem Produktpaket im Web Portal werden nun auch Bestellparameter übernommen, die am Produktpaket hinterlegt sind.	322296
Im Web Portal kann man nun in Hyperviews zoomen und sich bewegen.	367241

Verbesserung	Fehler ID
Im Web Portal kann man nun beim Attestieren einer Zuweisung eine Herkunftsanalyse durchführen.	388598
Im Web Portal kann man nun in der Attestierungshistorie für die Attestierung einer Zuweisung eine Herkunftsanalyse durchführen.	388599
Im Web Portal kann man nun Hyperviews per Klick so anzeigen, dass alle Informationen angezeigt werden.	418561
Bei Genehmigung oder Ablehnung einer Attestierung wird geprüft, ob eine Begründung angegeben werden muss.	415322
Hyperviews in Webanwendungen unterstützen nun die Anzeige von optischen Trennern.	206664
Das Web Portal und das Kennwortrücksetzungsportal unterstützen nun eine Darstellung, bei der die Kopf- und Menüleiste ausgeblendet werden.	404198
Als Verantwortlicher einer Anwendung kann man nun im Web Portal die Struktur der Servicekategorien für die Anwendung bearbeiten. Eine Leistungsposition mit Anwendungsberechtigung kann nur noch einer Servicekategorie unterhalb der Basisservicekategorie der Anwendung zugewiesen werden.	405217
Im Web Portal wurde ein neuer Menüpunkt **Verantwortlichkeiten > Meine Verantwortlichkeiten** hinzugefügt. Über diesen Menüpunkt kann man nun alle Objekte anzeigen, für die man verantwortlich ist.	406577
Im Web Portal wurde das Auflösen von Regelverletzungen in Complianceregeln für SAP Funktionen verbessert.	320932
Wenn sich Rollenmitgliedschaften eines angemeldeten Benutzers geändert haben, erhält dieser Benutzer im Web Portal eine entsprechende Benachrichtigung und muss sich neu anmelden.	293389
Wenn man im Web Portal ein Objekt für die weitere Bearbeitung oder die Detailansicht klickt, zeigt der sich öffnende Bereich nun den Namen des entsprechenden Objekts als Untertitel an.	303776
Falls der Konfigurationsparameter **MitigatingControlsPerViolation** aktiviert ist, kann der Bestellentscheider nun an den entstehenden Regelverletzungen einer Bestellung risikomindernde Maßnahmen hinzufügen, sofern er auch Ausnahmegenehmiger für die verletzte Regel ist. Zusätzlich kann der Anwender nun in der Bestellhistorie die risikomindernden Maßnahmen der Bestellung sehen.	305815
Falls der Konfigurationsparameter **MitigatingControlsPerViolation** aktiviert ist, kann man nun an Regelverletzungen risikomindernde Maßnahmen hinzufügen.	367357

Verbesserung	Fehler ID
Attestierungsläufe, die über einen Richtlinienverbund gestartet wurden, werden nun entsprechend im Web Portal gekennzeichnet.	316985
Im Web Portal kann man nun Bestellungen abbestellen, auf die man eine Schreibberechtigung hat.	36058, 319102
Die Verwaltung offener Attestierungsvorgänge wurde um folgende Punkte erweitert: • Anzeige der Nutzungsbedingungen am Attestierungsvorgang, sofern Nutzungsbedingungen an die zugrunde liegenden Attestierungsrichtlinie zugewiesen wurden • Anzeige der Richtlinienverletzungen des Basisobjekts des Attestierungsvorgangs • Attestierungsvorgänge mit Richtlinienverletzungen werden in der Übersicht optisch hervorgehoben • Anzeige der risikomindernden Maßnahmen für Richtlinienverletzungen eines Attestierungsvorgangs • Risikoanalyse für das Basisobjekt des Attestierungsvorgangs	319199
Im Web Portal kann man nun Richtlinienverletzungen risikomindernde Maßnahmen zuweisen.	319201
Im Web Portal wurde die Anzeige von ausgewählten Objekten vereinheitlicht.	320942
Das Auflösen von Regelverletzungen wurde um folgende Punkte erweitert: • Der Anwender kann eine Begründung angeben, die für die Abbestellung von Bestellungen verwendet wird, falls mindestens eine Abbestellung vorgenommen wird. • Erzeugte Abbestellungen werden in der Bestellhistorie so angezeigt, dass ersichtlich ist, wer die Auflösung der Regelverletzung ausgelöst hat. • Für Abbestellungen von Bestellungen wird automatisch eine Standardbegründung verwendet, die darauf hinweist, dass die Abbestellung zur Auflösung einer Regelverletzung vorgenommen wurde.	321559
Im Web Portal werden nun Hyperviews für folgende Objekte zur Verfügung gestellt: • Identitäten • Abteilungen • Anwendungsrollen • Geschäftsrollen	367240

Verbesserung	Fehler ID
• Kostenstellen • Standorte • Systemrollen • Benutzerkonten • Ressourcen • mehrfach bestellbare Ressourcen • mehrfach zu-/ abbestellbare Ressourcen • Zuweisungsressourcen • Systemberechtigungen • Complianceregeln • Unternehmensrichtlinien	
Im Web Portal kann man die Historie eines Objekts im Zeitstrahl anzeigen.	417844
Mithilfe des Kennwortrücksetzungsportals kann man nun ein neues Benutzerkonto erstellen.	387948
Im Web Portal kann man nun die Anhänge von Tickets verwalten (herunterladen, hochladen, bearbeiten und löschen) sowie die Ordnerstruktur der Anhänge bearbeiten.	388586
Im Web Portal kann man nun seinen eigenen Attestierungsstatus anzeigen.	388600
Die Anzeige des Empfängers einer Delegierung in der Bestellhistorie wurde verbessert.	36122, 388967
Die folgenden Programmfunktionen wurden eingeführt. • Portal_UI_ApplicationAdmin • Portal_UI_ApplicationOwner • Portal_UI_PAGStatistics • Portal_UI_PasswordHelpdesk • Portal_UI_PersonAdmin • Portal_UI_PersonManager • Portal_UI_PersonStatistics • Portal_UI_PolicyAdmin • Portal_UI_PolicyOwner • Portal_UI_PolicyStatistics • Portal_UI_QERPolicyAdmin • Portal_UI_QERPolicyStatistics	395043, 427871

Verbesserung	Fehler ID
• Portal_UI_ResourceAdmin • Portal_UI_RoleAdmin • Portal_UI_RoleStatistics • Portal_UI_RuleStatistics • Portal_UI_ShopAdmin • Portal_UI_ShopStatistics • Portal_UI_StructAdmin • Portal_UI_StructStatistics • Portal_UI_TSBStatistics	
An der Definition eines Parameters (für Berichte beziehungsweise für Bestellungen) kann man nun vorgeben, dass die Auswahl eines Parameterwertes aus einer flachen Liste (anstatt aus einem Baum) erfolgen soll.	307699
Im Web Portal für Betriebsunterstützung wurde die **Verfügbarkeitsprüfung** erweitert und überarbeitet.	205400
Im Web Portal für Betriebsunterstützung werden nur noch Objekte als ausstehend markiert, die direkt zugewiesen sind.	316548
Die Anzeige der Prozesse im Web Portal für Betriebsunterstützung wurde verbessert: • Man kann anhand der Prozess-ID direkt zu der Ansicht der Vorgänge gelangen, die zu dieser Prozess-ID gehören. • Man sieht für jeden Prozess einen zusammenfassenden Status. • Man kann die Liste der von einem Prozess betroffenen Objekte anzeigen. • Man kann die Fehlermeldung eines fehlgeschlagenen Prozessschritts anzeigen und diese in die Zwischenablage kopieren, um sie weiterzuverwenden.	327062
Im Web Portal für Betriebsunterstützung wurde das Verhalten für das Stoppen und Starten des Systems verändert, um die Abarbeitung der Queues möglichst verzögerungsfrei zu stoppen.	393858
Das Web Portal für Betriebsunterstützung wird nun nur noch angeboten, wenn eine Datenbankverbindung mit der Berechtigungsebene **Konfigurationsbenutzer** verwendet wird.	
Die Angular-Anwendungen verwenden nun Angular 14.	394843
Der RSTS wurde auf die Version 2023-02-28.1 aktualisiert.	404168

Verbesserung	Fehler ID
Änderungen: • Es können mehrere Instanzen des Dienstes nebeneinander installiert werden. • Integration von OneLogin MFA • Unterstützung für LDAPS mit SSL/TLS bei der Verbindung mit Active Directory oder einem LDAP-Server • Neue Unterstützung für die automatische Überwachung und Aktualisierung von Metadaten bei der Konfiguration mit einer URL • Entfernung von Starling 2FA Der RSTS muss für die Aktualisierung deinstalliert/neu installiert werden.	

Tabelle 4: Web Designer Webanwendungen

Verbesserung	Fehler ID
Aktualisierung der Drittanbieterkomponenten JQuery UI und Angular.js.	315799, 417517
Performanceverbesserungen im Web Designer Web Portal beim Anzeigen des Einkaufswagens.	33913, 430424
Beim Auflösen von Regelverletzungen im Web Designer Web Portal werden nun Begründung und Abbesteller für abbestellte Berechtigungen angeben.	35754
Die Sicherheit des Web Designer Web Portals wurde erhöht.	36328, 430932, 415297
Die Sicherheit beim Generieren von Berichten wurde erhöht.	37244

Tabelle 5: Zielsystemanbindung

Verbesserung	Fehler ID
Die Verwendung eines Verbindungszertifikats für die Anmeldung in Azure Active Directory wird unterstützt. Ein X.509 Zertifikat inklusive privaten Schlüssels wird benötigt. Die Verwendung eines selbstsignierten Zertifikats ist möglich. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36596 bereitgestellt.	36596
Als Eigentümer von Azure Active Directory Dienstprinzipalen können nun auch Dienstprinzipale zugewiesen werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35769 bereitgestellt.	35769

Verbesserung	Fehler ID
Die Liste der zulässigen Werte den bevorzugten Single Sign-On Modus für Azure Active Directory Dienstprinzipale wurde erweitert.	37198
Das Entfernen von Exchange Online Verteilerlisten ist jetzt auch möglich, wenn das Synchronisationsbenutzerkonto nicht als Manager an der Verteilerliste eingetragen ist.	36060
Der Exchange Online Konnektor verwendet und benötigt nun das Exchange Online Powershell Modul mit mindestens Version 3.2.0.	36363
Im Exchange Online Konnektor wurde die maximal konfigurierbare Anzahl von gleichzeitigen Verbindungen auf **999** erhöht.	36521
Der Konnektor für Azure Active Directory und Microsoft Teams verwendet jetzt die Version 5 des Microsoft Graph .NET SDKs (Graph Wrapper).	36738
Performanceverbesserung beim Laden bei Microsoft Teams Teams und Kanälen im Rahmen der Synchronisation.	33471
Für Microsoft Teams Teams wird die Option **Zulassen, dass Mitglieder private Kanäle erstellen** eingelesen und synchronisiert.	36568
Wenn ein Microsoft Teams Team archiviert wird, werden nun alle zugehörigen Eigenschaften mit Ausnahme der kundenspezifischen Spalten gesperrt und können nicht mehr bearbeitet werden.	36623
Die Konnektoren für Microsoft Exchange 2013, Microsoft Exchange 2016 und Microsoft Exchange 2019 unterstützen nun Zugriff auf die Eigenschaften `MessageCopyForSendOnBehalfEnabled` und `MessageCopyForSentAsEnabled`. Ein Mapping erfolgt im Standard nicht.	35784
Senden-als-Berechtigungen für Microsoft Exchange E-Mail-aktivierte Verteilergruppen werden unterstützt. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35776 bereitgestellt.	35776
OneLogin Rollen können nun automatisch in den IT Shop aufgenommen werden. Das Verhalten wird über den Konfigurationsparameter **QER | ITShop | AutoPublish | OLGRole** gesteuert.	35878
Für OneLogin Benutzerkonten kann nur angegeben werden, ob das Benutzerkonto gesperrt ist.	35989
Wenn für OneLogin Benutzerkonten ein genaueres Änderungsdatum bestimmt werden kann, wird der aktuelle Zeitstempel als Revisionsmerkmal verwendet.	37120
Für die Unterstützung von Behavior Driven Governance für One Identity Safeguard werden Prüfprotokolle synchronisiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch	36315, 36920

Verbesserung	Fehler ID
ID VPR#36315 bereitgestellt.	
Unterstützung von PAM Zugriffsanforderungen für Remote-Desktop-Anwendungen für Assets.	35731
Unterstützung von OneLogin als Authentifizierungsanbieter für PAM Benutzerkonten. Die Berichte und Richtlinien zur Nutzung der Multi-Faktor Authentifizierung wurden entsprechend angepasst.	35731
Unterstützung von PAM Zugriffsanforderungen für API-Schlüssel für Konten.	36617
Bereinigung der Synchronisationskonfiguration für SAP Berechtigungsobjekte. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35904 bereitgestellt.	35904
Im Objektfilter können SAP Benutzerkonten anhand des Merkmals `USTYP` gefiltert werden.	36427
Die Abbildung von Objekteigenschaften von SAP Rollen auf Systemberechtigungen im Unified Namespace wurde geändert. Es wird nun `SAPRole.RoleDescription` auf `UNSGroup.Description` abgebildet.	36498
Ein Synchronisationsprojekt für die Synchronisation von BI Analyseberechtigungen kann nur eingerichtet werden, wenn im SAP R/3-System die SAP Business Warehouse Komponente installiert ist.	36514
Bei Zuweisungen von Einzelrollen an Sammelrollen im SAP R/3-System werden nur als aktiv gekennzeichnete Mitgliedschaften synchronisiert.	36766
Beim Erstellen der Systemverbindung zu einer Cloud-Anwendung kann die Anzahl der Elemente pro Seite bei Anfragen für die Objektliste konfiguriert werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36376 bereitgestellt.	36376
Verbesserte Benutzerführung im Projektassistenten bei der Einrichtung der Synchronisation mit einer Cloud-Anwendung mit OAuth-Authentifizierung.	36905
Wenn eine Cloud-Anwendung den Zugriff auf das Zielsystem bei zu vielen Anfragen sperrt, versucht der SCIM-Konnektor nach einer Wartezeit die Anfragen erneut zu senden. Dabei werden Definitionen gemäß RFC 6585 beachtet. Der Konnektor führt bis zu 30 Wiederholversuche aus.	36339
Der SCIM Konnektor erlaubt kundenspezifische Header-Zeilen bei GET-Anfragen.	36202
Bei der Authentifizierung des SCIM Konnektors über OAuth werden die konfigurierten Daten zu Client-ID und Client-Secret immer im Header und	36912

Verbesserung	Fehler ID
im Body des `POST`-Request übertragen.	
Der One Identity Manager Konnektor stellt eine virtuelle Schemaeigenschaft bereit, mit der die Übersetzungen von Einzelwerten gemappt werden können.	36375
Beim Einrichten der Synchronisation mit dem CSV Konnektor kann der Pfad zur CSV-Datei als absoluter Pfad oder als relativer Pfad zur CSV-System-datei angegeben werden. So können CSV-Dateien aus unterschiedlichen Speicherorten in einem Synchronisationsprojekt verwendet werden.	35420
Bei der Konsistenzprüfung von Powershell Konnektor-Definitionen wird nun geprüft, ob für eine laut Definition lesbare Eigenschaft auch mindestens ein Rückgabekommando (ReturnBinding) definiert wurde.	35654
Erweiterte Protokollierungsmodi bei Ausführung von Windows PowerShell Skripten mit PowershellComponentNet4.	36811
Das neue Format der ClientSecret-Strings, die von One Identity Starling Connect generiert werden, wird unterstützt.	36156
Verbesserte Fehlerbehandlung für Zielsystemkonnektoren, die den lokalen Cache nutzen, wenn einzelne Objekte aufgrund fehlerhafter Daten nicht geladen werden können.	36793
Der Wert von Variablen für Quotas kann auch als Prozentzahl angegeben werden.	36510
Performanceverbesserung beim Erstellen von Anzeigewerten für Synchronisationsobjekte.	36284
Im Zielsystembrowser gibt es die Möglichkeit einen bereits definierten Filter für die Ergebnisliste zu bearbeiten.	36154
Der Dialog für die Entschlüsselung von Verbindungsdaten im Synchronization Editor wurde verbessert.	36026
Im Dialog zur Auswahl des Synchronisationsservers kann nun auch ein bereits vorhandener Jobserver ausgewählt werden. Diesem Jobserver wird die passende Serverfunktion automatisch zugewiesen.	35903
Wenn im Manager auf dem Formular **Zielsystemabgleich** eine Methode zur Behandlung der ausstehenden Objekte aufgrund von Einschränkungen nicht ausgeführt werden kann, dann ist das jeweilige Symbol deaktiviert. Details über die jeweilige Einschränkung können angezeigt werden.	31890
Neue Konsistenzprüfung für Synchronisationsprojekte, die vor Konfi-gurationsfehlern in Mappings von M:all-Tabellen (beispielsweise `ESetHasEntitlement`) warnt.	36666
Beim Anlegen, Ändern und Löschen von Benutzerkonten in kunden-	36989

Verbesserung	Fehler ID
definierten Zielsystemen (`UNSAccountB`) werden nicht benötigte Nachberechnungsaufträge vermieden.	
Neuer Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** mit dem als ausstehend markierte Benutzerkonten automatisch gelöscht werden.	32052
Im Manager wird auf den Formular **Suchkriterien für die Identitätenzuordnung definieren** an den Zielsystemen jetzt zusätzlich der Aktivierungszustand der Identitäten und Benutzerkonten angezeigt. Es wird eine Option angeboten, auch gesperrte Benutzerkonten manuell mit Identitäten zu verbinden.	32254
Im Manager können auf den Stammdatenformularen für Benutzerkonten der Zielsysteme nun auch inaktive Identitäten an Benutzerkonten zugewiesen werden. Über den neuen Konfigurationsparameter **QER | Person | HideDeactivatedIdentities** wird definiert, ob inaktive Identitäten auf den Stammdatenformularen für Benutzerkonten ein- oder auszublenden sind.	36703, 36734
Verweise auf die Active Directory Edition wurden aus dem Installationsassistenten und aus den Handbüchern entfernt. Bestehende Installationen dieser Edition sind nicht beeinträchtigt.	36939
Im Manager werden auf den Überblicksformularen für Benutzerkonten die Informationen zur Vererbbarkeit von Systemberechtigungen besser dargestellt.	36049

Tabelle 6: Identity Management und Access Governance

Verbesserung	Fehler ID
Nutzungsbedingungen können als PDF-Datei in verschiedenen Sprachen bereitgestellt werden.	31889
Für einen Attestierungsvorgang werden die Informationen zum Attestierungsobjekt über einen Bericht oder als Snapshot bereitgestellt. Bericht und Snapshot können im Manager angezeigt werden.	35498
Diverse Verbesserungen bei der Ermittlung der Attestierer mit dem Entscheidungsverfahren **SO**.	36477
Wenn im Genehmigungsverfahren für Bestellungen Complianceregelverletzungen ermittelt werden, können die Ausnahmegenehmiger bei der Genehmigung der Regelverletzung risikomindernde Maßnahmen zuweisen.	21081
An der Tabelle `ComplianceRule` wurden verschiedene Spalten zusätzlich als mehrsprachig gekennzeichnet. Deren Inhalt kann nun übersetzt werden.	36845
Umbau des Regeleditors für Complianceregeln für zukünftige	35131

Verbesserung	Fehler ID
Erweiterungen. Diese Änderung entfernt den Assembly-Wert in der XML-Konfiguration. Regelbedingungen, die mit älteren One Identity Manager-Versionen erstellt wurden, können weiterhin gelesen werden. Complianceregeln, die mit One Identity Manager 9.2 erstellt werden, funktionieren nicht in älteren One Identity Manager-Versionen.	
Für das Akzeptieren von Nutzungsbedingungen kann eine Multifaktor-Authentifizierung angefordert werden.	35859
Fehlermeldungen des IT Shop-Customizers verwenden kundenspezifische Anzeigewerte und Datumsformate und können übersetzt werden.	36053
An dauerhaft deaktivierte Identitäten werden keine E-Mail-Benachrichtigungen mehr versendet.	36152
Attestierer von Leistungspositionen sehen auf dem Überblicksformular von Leistungspositionen alle Informationen über das Attestierungsobjekt.	36173
Auf dem Überblicksformular einer Anwendungsrolle werden auch die Entscheidungsworkflows angezeigt, in denen die Anwendungsrolle als Fallback-Entscheider ermittelt wird.	36213
Stellvertretungen und Delegierungen werden beendet, wenn der Stellvertreter deaktiviert wird.	36300
Die Anzeigewerte einiger Werte der Spalte `AttestationHistory.DecisionType` wurden korrigiert, sodass der Anzeigewert und die englische Übersetzung des Anzeigewertes identisch sind.	36460

Wert	Bisheriger Anzeigewert	Neuer Anzeigewert
Abort	Aborted	Canceled
Direct	Direct	Forward
RevokeAdditional	RevokeAdditional	Revoke additional approver

Wenn Sie in kundenspezifischen Skripten, beispielsweise für E-Mail-Benachrichtigungen, die Übersetzungen der Anzeigewerte ermitteln, dann passen Sie diese Skripte entsprechen an. Nutzen Sie den neuen Anzeigewert als Schlüssel für die Übersetzung.

Beispiel bei Verwendung im Prä-Skript zur Generierung eines Prozesses:

- Bisher: `Connection.MultiLanguage.GetInLanguage ("AttestationHistory", "DecisionType", "Abort", personLanguage).ToString()`
- Neu: `Connection.MultiLanguage.GetInLanguage`

Verbesserung	Fehler ID
`("AttestationHistory", "DecisionType", "Canceled", personLanguage).ToString()`	
Die Anzeigewerte einiger Werte der Spalte `PWODecisionHistory.DecisionType` wurden korrigiert, sodass der Anzeigewert und die englische Übersetzung des Anzeigewertes identisch sind.	36460

Wert	Bisheriger Anzeigewert	Neuer Anzeigewert
Abort	Abort	Cancel
AddAdditional	AddAdditional	Additional approver
AddHistoryEntry	AddHistoryEntry	Show in history
AddInsteadOf	AddInsteadOf	Delegation
ChangeBoard	ChangeBoard	Change shelf
CreateOrder	CreateOrder	Stock request
Grant	Grant	Approval
ResetReservation	ResetReservation	Reset reservation
RevokeAdditional	RevokeAdditional	Revoke additional approver
RevokeDelegation	RevokeDelegation	Revoke delegation

Wenn Sie in kundenspezifischen Skripten, beispielsweise für E-Mail-Benachrichtigungen, die Übersetzungen der Anzeigewerte ermitteln, dann passen Sie diese Skripte entsprechen an. Nutzen Sie den neuen Anzeigewert als Schlüssel für die Übersetzung.

Beispiel bei Verwendung in einem Skript:

- Bisher: `multiLanguage.Get("PWODecisionHistory", "DecisionType", "Grant")`
- Neu: `multiLanguage.Get("PWODecisionHistory", "DecisionType", "Approval")`

Auf dem Überblicksformular einer Bestellung werden die verwendeten Bestelleigenschaften (moderne Definition) und ihre Parameter angezeigt.	36652
Im Bericht **Bestellhistorie** für eine Identität werden genehmigte mehrfach bestellbare Ressourcen jetzt unter dem Tabreiter **Genehmigte mehrfach bestellbare Ressourcen** angezeigt.	36654
Optimierung der Berechnung von SAP Funktionen.	36796

Verbesserung	Fehler ID
Für die zeitweilige Deaktivierung einer Identität kann nun ein Grund erfasst werden. Dafür wurde an der Tabelle `Person` die Spalte `LeaveofAbsenceReason` (**Grund der Abwesenheit**) eingefügt.	35739
Performanceverbesserungen bei der Berechnung von SAP Funktionen.	36821
In der Berechtigungsdefinition von SAP Funktionen können maskierte Sonderzeichen verwendet werden.	36780
Performanceverbesserung bei der Prüfung der Bedingung von Attestierungsrichtlinien.	37134
Verbesserte Darstellung des Dialogs **Produkte verschieben** im Manager.	36636
Die folgenden Skripte zur Bildung von Links in E-Mails für die direkte Entscheidung von Bestellungen oder zur direkten Attestierung oder zur Anzeige von Regelverletzungen wurden intern umgestellt auf Nutzung von `IEntity`. • VI_BuildITShopLinks • VI_BuildAttestationLinks • VI_BuildComplianceLinks Sollten diese Skripte kundenspezifisch für andere Einsatzzwecke als für Mailvorlagen genutzt werden, so muss der Aufrufparameter von `Base` zu `Entity` geändert werden.	36556
Die Berechnung der zulässigen Entscheider im Entscheidungsworkflow wurde optimiert. Bereits abgeschlossene Entscheidungsebenen werden nicht mehr bei jeder Änderung nachberechnet.	35602
Die Programmfunktion **ApplicationStart_ApplicationGovernance** wird nicht mehr benötigt und wurde entfernt.	35869
Die Entscheidungsverfahren **OA** und **TO** wurden erweitert, um Entscheider für Zuweisungsbestellungen zu ermitteln. Das Entscheidungsverfahren **EN** wurde erweitert, um Attestierer für Zuweisungen von Systemberechtigungen an hierarchische Rollen zu ermitteln.	36432
Wenn eine E-Mail-Benachrichtigung aus dem IT Shop aufgrund eines Verarbeitungsfehlers nicht versendet werden kann, wird der Absender dieser E-Mail informiert und die ursprüngliche E-Mail aus dem Postausgang gelöscht. Es wird eine neue Mailvorlage **Genehmigung - Fehler bei der Verarbeitung einer Genehmigungsmail** bereitgestellt.	21300, 31884
Bei der Berechnung des Peer-Gruppen-Faktors werden auch mehrfach bestellbare Ressourcen berücksichtigt.	35854

Siehe auch:

- Schemaänderungen auf Seite 54
- Patches für Synchronisationsprojekte auf Seite 63

Gelöste Probleme

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

Tabelle 7: Allgemein

Gelöstes Problem	Fehler ID
Im Mailvorlageneditor werden unter Umständen Hyperlinks nicht vollständig angezeigt.	35676
In seltenen Fällen wurde bei der Prozessverarbeitung versucht, den identischen Prozess mehrfach in die Prozessanzeige (Tabelle `DialogProcess`) einzutragen, was zu einer Primärschlüsselverletzung und damit zum Fehler führte.	35765
Fehler im Where-Klausel-Assistenten bei der Anzeige von Datumsangaben mit **Null**-Werten.	35801
Beim Bearbeiten der Verbindungszeichenkette im Verbindungsdialog wird die erste Änderung nicht übernommen.	35911
In seltenen Fällen tritt beim Ausführen von Datenbankabfragen durch die Objektschicht ein Fehler auf. Fehlermeldung: `the Size property has an invalid size of 0`	35993
Bei der Installation oder Aktualisierung des One Identity Manager wurden kundenspezifische Dateien im falschen Unterverzeichnis gespeichert.	36054
Im Designer ist im Skripteditor die Auswahlliste für Skripte zu schmal.	36085
Ein Fehler bei der Markierung eines abgearbeiteten Prozessschritte für das Löschen oder die Archivierung.	36098
Fehler bei der Installation des Anwendungsservers aufgrund von Abhängigkeiten zu Microsoft Edge WebView2.	36107
Im Configuration Wizard wird nicht der administrative Benutzer verwendet, der auf der Seite **Systemadministrator-Berechtigung** ausgewählt wird.	36248
Kumulative Transportpakete werden in der Transporthistorie nicht korrekt angezeigt.	36260
Für das Erstellen und Einrichten einer One Identity Manager-Datenbank wird ein Installationsbenutzer mit einer Serverrolle **dbcreator** vorausgesetzt, selbst wenn eine bereits vorher erstellte Datenbank genutzt	36295

Gelöstes Problem	Fehler ID
werden soll.	
Prozessabholung über den **HttpJobProvider** funktioniert nicht, wenn für den Proxyserver die Nutzung von SSL konfiguriert ist.	36329
Im Designer können im Schemaeditor Spaltendefinitionen nicht geladen werden, wenn diese über eine Präprozessorbedingung deaktivert sind.	36340
Inkonsistenzen in der Definition der Abhängigkeiten von DBQueue Prozessor-Aufträgen.	36366
Im Designer wird im Wörterbucheditor der Datenquelle eines Schlüsselwertes nicht korrekt befüllt.	36402
Bei der Prozessersetzung im DBQueue Prozessor bleiben unter Umständen Einträge bestehen, die auf einen nicht mehr vorhandenen Prozess verweisen.	36645
Beim Wechseln des Parametertyps von Berechnung auf Benutzerabfrage wird die Spalte **Tabellenspalte (kalk.)** für den Parameter (`DialogParameter.UID_DialogColumnCalculate`) nicht geleert.	36664
Fehlerhafte Anzeige von historischen Zuordnungen in Berichten, wenn eine Datenbanksicht als Tabelle verwendet wird.	36695
Wenn während der Komprimierung von DBQueue Prozessor-Aufträgen der Database Agent Service beendet wird, kommt es zum Datenverlust.	36708
Der Sprachcode **nb** fehlt.	36714
Fehlerhafte Umwandlung von Zeitwerte mit dem Zeitanteil `00:00` und dem Datumsformat `DateTime`.	36745
In der Dokumentation zum Docker-Container für den One Identity Manager Service ist der Parameter `CONFIGFROMDB` unzureichend beschrieben.	36779
Unter Umständen kann es nach Aktualisierung verwaiste Einträge für gelöschte Maschinenrollen in der Datei `ModuleInfo.xml` des Moduls **CCC** geben.	36810
Gelegentlich tritt in der Übersicht über die Systemkonfiguration ein Fehler auf. Fehlermeldung: `Divide by zero error encountered.`	36822
Im One Identity Manager Installationshandbuch fehlt Port 443 in der Liste der Kommunikationsports.	36851
Die Erstellung von Watch-Triggern schlägt fehl, wenn eine Spalte für verschiedene Datenbanksichten zur Aufzeichnung von Datenänderungen markiert ist und die Sichten auf derselben Basistabelle basieren.	36857

Gelöstes Problem	Fehler ID
In seltenen Fällen wurde ein Zeitplan mehrfach ausgelöst.	36861
Der Database Compiler bleibt bei der Bestimmung der Compiler-Tasks stehen.	36865
Im Designer tritt beim Zuweisen von Berechtigungsgruppen zu Anwendungen ein Fehler auf. Fehlermeldung: `Object reference not set to an instance of an object.`	36879
Bei der Berechnung des Anzeigemusters tritt ein Fehler auf, wenn verschiedene Datentypen verwendet werden. Fehlermeldung: `Conversion failed when converting the nvarchar value '<value>' to data type int.`	36895
Die Anmeldung an der Manager Webanwendung ist nicht möglich, wenn sich der Benutzer in der Zeitzonen mit UTC+00:00 befindet.	36901, 431158
Beim Transport mit Änderungskennzeichen werden Beschreibung und Kommentar des Änderungskennzeichens nicht mit übertragen.	36904
In Berichten, die mit dem Report Editor erstellt wurden, enthalten Filter und Zusammenfassungen falsche Ergebnisse.	36906
Der Vergleich von Spalten mit Datums- und Zeitwerten funktioniert nicht immer korrekt.	36945
Fehler bei der Verarbeitung von Prozessen, welche die Prozessfunktion `ModifyFileAccess_Universal` nutzen. Fehlermeldung: `Cacls.Exe failed with return code 122 ("The data area passed to a system call is too small").` HINWEIS: Die Prozessfunktion wurde in Standardprozessen durch die Prozessfunktion `ModifyFileAccess_DotNet` ersetzt. Weitere Informationen finden Sie unter Neue Funktionen auf Seite 2.	36946
Bei der Aktualisierung von One Identity Manager Version 8.x auf eine höhere Version tritt beim Kompilieren des typsicheren Datenbankmodells unter Umständen ein Fehler auf. Fehlermeldung: `Keyword is not valid as an identifier.`	36949
Fehler beim Speichern einer Objektänderung im Manager als geplante Operation, wenn der Manager über einen Anwendungsserver gestartet wurde.	36951
Einträge in der Jobqueue werden zu oft zur Neuberechnung markiert. Dadurch wird die Verarbeitung der Jobqueue blockiert. Der DBQueue Prozessor-Auftrag `QBM-K-JobqueueOverviewInvalid` wurde jetzt durch einen Trigger ersetzt.	36962, 36963

Gelöstes Problem	Fehler ID
Performanceprobleme beim Prüfen mehrspaltiger Eindeutigkeiten, wenn massenhaft Objekte in die One Identity Manager-Datenbank eingefügt werden.	37027
In der Manager Webanwendung können keine SAP Rollen an SAP Benutzerkonten zugewiesen werden.	37032, 431268
Fehler beim Import von Daten in die Tabelle `QBMDBPrincipal`, wenn dadurch doppelte Einträge bezüglich Datenbankbenutzer oder Anmeldename entstehen.	37045
Neuberechnungsaufgaben für den DBQueue Prozessor, die sich auf das Zielsystem Basismodul (TSB) beziehen, werden unter Umständen nicht automatisch ausgelöst.	37048
Fehler beim Anzeigen des Prozesses `QBM_TransportToHistoryDatabase` im Prozesseditor, wenn die Serverfunktion **SQL Ausführungsserver** an mindestens zwei Jobserver zugewiesen ist.	37050
Änderungen an Bildungsregeln oder Formatskripten im Designer werden mitunter nicht in die Datenbank gespeichert.	37056
Beim Öffnen einer Kennwortrichtlinie im Designer wird eine falsche Warnung angezeigt.	37083
Fehler, wenn `DialogDatabase.EditionDescription` als `isBlobExternal` gekennzeichnet ist.	37108
Filter, die im SCIM-Konnektor generiert werden, haben unter Umständen eine nicht-benötigte Klammerebene. Einige SCIM-Anbieter geben aufgrund dieser Filter den Status `Bad request` zurück.	37119
Die Ansicht der Änderungshistorie eines Objektes kann unter Umständen das Limit von 8000 Elementen einer In-Klausel überschreiten.	37140

Tabelle 8: HTML-Webanwendungen

Gelöstes Problem	Fehler ID
Im Web Portal werden im Einkaufswagen nicht die korrekten Produktnamen verwendet.	35818, 317017
Im Web Portal werden zur Auswahl stehende Sprachen nicht in der entsprechenden Sprache angezeigt.	36138
Der Docker-Container für den API Server protokolliert nicht nach Application Insights.	36484
Der Index im Web Portal gerät in eine Endlosschleife.	36587
Wenn bei der Abfrage eines Bestellparameters im Web Portal außerhalb des Fensters geklickt wird, wird der Bestellvorgang abgebrochen.	36813

Gelöstes Problem	Fehler ID
Im Web Portal kommt es beim Prüfen des Einkaufswagens zum Fehler, wenn das bestellte Produkt einen Bestellparameter hat, der eine Liste zulässiger Werte enthält.	36847, 431117
Im Administrationsportal kommt es beim Speichern globaler Änderungen zum Fehler.	36848, 431121
Beim Genehmigen von Delegierungen kommt es zum Fehler, wenn eine benutzerdefinierte Entscheidungsrichtlinie verwendet wird.	36854, 416803
Fehler bei der Prüfung von Bestellparametern im Einkaufswagen, wenn der Parameter eine einschränkende Bedingung mit einer Variablen enthält.	36878
Im Web Portal funktioniert das Hinzufügen von Produkten zum Einkaufswagen nicht.	37144
Im Web Portal wird im Workflow einer Bestellung das Zurückziehen eines zusätzlichen Entscheiders falsch angezeigt.	292577
Wenn man versucht sich mit einem abgelaufenen Zugangscode am Kennwortrücksetzungsportal anzumelden, erhält man falsche Informationen.	305015
Unter bestimmten Umständen wird im Web Portal die Prüfung auf Regelverletzungen für Zuweisungsbestellungen nicht angezeigt.	306828
Unter bestimmten Umständen wird im Web Portal beim Genehmigen eines Attestierungsvorgangs eine Fehlermeldung angezeigt.	317836
Wenn man im Web Portal neue Bestellungen über Peer-Gruppen oder Referenzbenutzer ausführt, werden die Produkte, die über Organisationsstrukturen gewählt werden, nicht in den Einkaufswagen gelegt.	319781
Unter bestimmten Umständen werden im Web Portal beim Bearbeiten von Attestierungsrichtlinien die Bedingungen der Attestierungsrichtlinie gelöscht.	320926
Im Web Portal kann der Bericht **Vergleich des Zugangs von Identitäten** nicht generiert werden.	322252
Unter bestimmten Umständen funktioniert die Suchfunktion im Web Portal nicht und erzeugt einen Fehler.	327287
Im Web Portal werden zu einem Produkt, das bei der Bestellung zu einer Regelverletzung führt, nicht alle Details über die Regelverletzung angezeigt.	331942
Im Administrationsportal werden die Werte **true** und **false** nicht übersetzt.	386304
Shops, die Shoppingcentern zugewiesen sind, werden im Web Portal nicht in der Liste der bearbeitbaren Shops angezeigt.	403983

Gelöstes Problem	Fehler ID
Der API Server erstellt für jede Anfrage eine neue Sitzung, wenn derselbe Authorisierungstoken verwendet wird.	405848
Bestellparameter vom Typ `query` werden nur korrekt behandelt, wenn die Abfragespalte entweder `XObjectKey` oder eine Primärschlüsselspalte ist.	412932
Die Registrierung eines neuen Benutzers im Kennwortrücksetzungsportal schlägt fehl.	415340
Im Web Portal können Delegierungen ohne zeitliche Befristung erstellt werden.	416793
Die Suche im Administrationsportal geht nicht korrekt mit Groß- und Kleinschreibung um.	418578
In der Prozessansicht im Web Portal für Betriebsunterstützung werden alle Prozessschritte eines Prozesses mit dem selben Namen angezeigt.	419792
Im Web Portal für Betriebsunterstützung werden die vorhandenen Jobqueue-Aufträge nur mit Verzögerung angezeigt.	426530

Tabelle 9: Web Designer Webanwendungen

Gelöstes Problem	Fehler ID
In der `VI_Edit_Multiselect`-Komponente des Web Designer kann kein Wert abgewählt werden.	36558
Das Anzeigen der Stammdaten einer Identität im Web Designer Web Portal erzeugt einen Fehler.	36578, 405073
Im Web Designer Web Portal ist es nicht möglich, ein Produkt abzubestellen.	36647
Im Web Designer Web Portal werden für die Werte in manchen Auswahllisten keine Übersetzungen angezeigt.	36761, 414583
Im Web Designer Web Portal wird bei der Prüfung des Einkaufswagens keine Regelverletzung ermittelt, obwohl Pflichtparameter nicht angegeben wurden.	36764, 431063
Nach Abmeldung vom Web Designer Web Portal funktioniert die Weiterleitung zur konfigurierten URI nicht, wenn in der OAuth/OpenID Connect Konfiguration **Weiterleitungs-URI für die Anwendung senden** konfiguriert ist.	36874
Wenn ein Genehmiger eine Bestellung im Web Designer Web Portal über einen Link öffnet und genehmigt, wird ein vorhandenes Gültig-bis-Datum gelöscht.	37121, 431359
Code, der in benutzerdefinierte Funktionen des Web Designer kopiert wird, wird umformatiert.	428028

Gelöstes Problem	Fehler ID
In der Web Designer-Komponente `VI_Edit_Special_Person_TemporaryDeactivated` kann der Parameter `IsTemporaryDeactivated` nicht auf **readonly** gesetzt werden.	430791

Tabelle 10: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Bei der Behandlung von ausstehenden Exchange Online E-Mail Benutzern werden unnötige Provisionierungsaufträge für Azure Active Directory Gruppen erzeugt.	36707
Fehler bei der Synchronisation mit dem generischen Datenbankkonnektor, wenn der Synchronisationsserver auf einem Linux Server eingerichtet ist. Fehlermeldung: `The time zone ID 'FLE Standard Time' was not found on the local computer.`	34451
Fehler bei der Synchronisation mit dem One Identity Manager Konnektor, wenn in gleichnamigen Schematypen gleichnamige virtuelle Schemaeigenschaften verwendet werden. Fehlermeldung: `Error compiling synchronization project. An item with the same key has already been added.`	35811
Verschiedene Eigenschaften vorn OneLogin Benutzerkonten werden bei jeder Synchronisation geändert.	35958
Performanceprobleme bei der Synchronisation einer SharePoint Online-Umgebung mit sehr vielen Websitesammlungen.	35975
Im Launchpad kann ein Endbenutzer (Datenbankbenutzer) den Offlline-Modus für ein Zielsystem nicht aktivieren.	36007
Fehler beim Lesen von Daten mit dem CSV Konnektor, wenn eine Remoteverbindung zum CSV-System besteht.	36126
Konvertierungsfehler beim Anzeigen von Azure Active Directory Objekten im Zielsystembrowser. Fehlermeldung: `[1777022] Schema property (extension_<guid>_description@User) only accepts data of type (System.String). The value loaded (["<user>"]) is however type (System.Text.Json.JsonElement).`	36306
Mitgliedschaften in Systemberechtigungen, die als ausstehend markiert sind, sind im One Identity Manager wirksam. Damit können diese Systemberechtigungen im One Identity Manager nicht gelöscht werden.	36395
Wenn in der Schemaerweiterungsdatei für ein SAP R/3-Schema eine Funktion mit optionalen Parametern definiert ist, dann haben die Einzelobjekte bei der Synchronisation leere Eigenschaften. Im Zielsystembrowser sind die Eigenschaften jedoch korrekt befüllt.	36425

Gelöstes Problem	Fehler ID
Im One Identity Manager Administrationshandbuch für die Anbindung Unix-basierter Zielsysteme sind die minimalen Berechtigungen unzureichend beschrieben.	36435
`Insert`-Operationen dauern ungewöhnlich lange, wenn der SCIM-Provider keine Suche mit Einsatz von Filtern auf den Endpunkten unterstützt.	36459
Wenn im One Identity Manager die Zuweisung einer BI Analyseberechtigung an ein BI Benutzerkonto gelöscht wird, dann entfernt der Provisionierungsprozess die Zuweisung nicht aus dem SAP R/3-System.	36517
Im One Identity Manager Password Capture Agent Administration Guide fehlt die Beschreibung des Parameters `DeleteJob`.	36592
Im One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung sind die Berechtigungen zur Nur-App-Authentifizierung über ein selbstsigniertes Zertifikat unzureichend beschrieben.	36619
Wenn mehrere Synchronisationsprojekte für ein Zielsystem vorhanden sind, werden die Provisionierungsaufträge gegebenenfalls für das falsche (inaktive) Projekt erzeugt.	36671
Wenn ein Microsoft Teams Team archiviert wird, bleibt die zugehörige SharePoint Online Seite weiterhin bearbeitbar.	36677
Im One Identity Manager Administrationshandbuch für die Anbindung einer Microsoft Exchange-Umgebung sind die benötigten Berechtigungen unvollständig beschrieben.	36680
Die Zuweisungen von SAP Benutzerkonten zu SAP Rollen werden nicht korrekt aktualisiert, wenn die Struktur der SAP Rollen geändert wird.	36701
Bei Verwendung des PowerShell Moduls v3 kann es zu einem Fehler bei der Synchronisation mit Exchange Online kommen. Fehlermeldung: `You must call Connect-ExchangeOnline before calling any other cmdlet.`	36709, 37137
Beim erneuten Anwenden der Bildungsregeln für E-Mail-aktivierte Azure Active Directory Gruppen werden die Spalten `AADGroup.IsSecurityEnabled` und `AADGroup.IsMailEnabled` geändert.	36713
Die Kommunikationsdaten von SAP Benutzerkonten werden aus Systemen mit Geschäftspartner-Funktionalität nicht korrekt gelesen, wenn das Benutzerkonto mit einer HCM Person verbunden ist (identische Personalnummer) und jeweils eigene Adress- und Kommunikationsdaten existieren.	36754
Fehler, wenn in der Zentraldatenbank von Synchronisationsprojekten für	36755

Gelöstes Problem	Fehler ID
die Systemsynchronisation auf Schemaeigenschaften, die M:N Schematypen oder Schlüsselauflösungen abbilden, zugegriffen wird. Fehlermeldung: `The system (...) does not have a data store.` Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36755 bereitgestellt.	
Für bestimmte Typen von SAP R/3 Schemaerweiterungen kann es vorkommen, dass im Zielsystembrowser alle Eigenschaften der Objekte dieses Schematyps korrekt gelesen werden, aber während der Synchronisation nicht auf alle Eigenschaften zugegriffen wird.	36768
Fehlende Customizer für OneLogin Benutzerkonten (Tabelle `OLGUser`).	36771
Wenn bei der Ausführung eines Skripts mit der Prozessfunktion `ExecuteScript` der Prozesskomponente `PowerShellComponentNet4` der Wert **$null** zurückgegeben wird, tritt ein Fehler auf. Fehlermeldung: `Object reference not set to an instance of an object.`	36776
Das Skript `OLG_PersonAuto_Mapping_OLGUser` verweist auf eine nicht vorhandene Spalte. Fehlermeldung: `Column UID_TSBAccountDefUser does not exist.`	36788
Die Zuweisung der Gruppenmitgliedschaft in einem AIX-System ohne Berechtigung zur Verwendung des Befehls `bin/mv` schlägt fehl.	36794
Fehler bei der Synchronisation der Eigentümer von Azure Active Directory App-Registrierungen, wenn der Eigentümer ein Dienstprinzipal ist. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36799 bereitgestellt.	36799
Fehler beim Laden eines Synchronisationsprojekts. Fehlermeldung: `[System.TypeLoadException] Method 'TryConvertFromString' not found.`	36815
Fehler bei der Synchronisation von Notes Admin4-Datenbanken und Zertifikatsanforderungen. Fehlermeldung: `Error running synchronization step (AdminRequest) of synchronization configuration (Initial Synchronization). Quota (2) exceeded for method (Delete object).` Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36831 bereitgestellt.	36831
Während der Delta-Synchronisation wird der Gruppentyp von Azure Active Directory Gruppen nicht korrekt eingetragen.	36840
Die Provisionierung von Active Directory Gruppen schlägt sporadisch fehl, wenn Mitgliedschaften und das Mitglied gleichzeitig gelöscht werden.	36843

Gelöstes Problem	Fehler ID
Fehler bei der Synchronisation einer SAP R/3-Umgebung, wenn die Synchronisationskonfiguration eine Schemaerweiterung enthält, welche in der Tabellendefinition eine Where-Klausel verwendet, die länger als 72 Zeichen ist.	36869
Verbindungsfehler im SCIM Konnektor, wenn eine Authentifizierung auf Basis eines Client-Zertifikats verwendet wird, obwohl das Zertifikat als korrekt validiert wurde.	36872
Auf dem Überblicksformular für Azure Active Directory Benutzerkonten werden inaktive Gruppenmitgliedschaften angezeigt.	36899
Das Laden eines Benutzerkontos ohne Foto in Azure Active Directory kann zu einer Fehlermeldung `ImageNotFound` führen.	36928
Beim Laden fehlerhafter SAP Benutzerkonten bricht die Synchronisation ab, statt die fehlerhaften Objekte zu protokollieren und die Synchronisation fortzusetzen.	36931
Unter Umständen schlägt die Active Directory Synchronisation fehl mit der Meldung: `Value cannot be null.`	36938
Werden Buchungsberechtigungen für ein Objekt bearbeitet, auf dem im Microsoft Exchange noch ein Element steht, welches selbst kein Empfänger mehr ist, kommt es zum Fehler `You cannot call a method on a null-valued expression.`	36953
Das Lesen der Eigenschaft `Tenant.AllowedDomainListForSyncClient` schlägt fehl, wenn Daten zu dieser Eigenschaft im SharePoint Online vorhanden sind. Fehlermeldung: `Object cannot be stored in an array of this type.`	36956
Fehler bei der Synchronisation einer SharePoint Online-Umgebung, wenn eine Websitesammlung sehr viele Websites enthält. Fehlermeldung: `Die Anforderung verwendet zu viele Ressourcen.` Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36961 bereitgestellt.	36961
Bei der Synchronisation einer SAP R/3-Umgebung mit Revisionsfilterung werden nicht nur die geänderten Benutzerkonten geladen, sondern alle. Fehlermeldung: `Object list of type USER is not able to read property BAPIUCLASS~SYSID. Subsequent loading of all single objects will affect performance.` Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36970 bereitgestellt.	36970
Beim Laden eines SCIM Schemas mit Schemaerweiterungen ist die Liste der Namen der genutzten Schemaerweiterungen leer.	36985

Gelöstes Problem	Fehler ID
Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#36985 bereitgestellt.	
Fehler im generischen Datenbankkonnektor für Oracle Database beim Auslesen von großen Zahlenwerten aus einer Tabellenspalte des Typs `NUMBER(20)`. Fehlermeldung: `Arithmetic operation resulted in an overflow`	36993
Fehler beim Laden von Objekten des Schematyps `ExternalEmail`, wenn einer Google Workspace Gruppe der komplette Google Workspace Kunde als Mitglied zugewiesen ist.	37024
Fehler beim Starten einer Provisionierung, wenn es für das geänderte Objekt Objektreferenzen gibt, die bei der Synchronisation ignoriert wurden. Fehlermeldung: `Unable to cast object of type 'System.Byte[]' to type 'System.IComparable'.`	37031
Fehlerhafte Konvertierung von Datumswerten im generischen Datenbankkonnektor.	37037
Fehler im CSV Konnektor bei der Behandlung von Objektreferenzen.	37039
Bei der Synchronisation von Mitgliedschaften wird der Synchronisationspuffer nicht bereinigt, wenn an der Wertevergleichsregel **Groß-/Kleinschreibung ignorieren** aktiviert ist.	37062
Auf dem Stammdatenformularen der Benutzerkonten werden die Werte in der Eigenschaft **Kategorie** nicht korrekt angezeigt.	37070
Die Delta-Synchronisation von Azure Active Directory Benutzerkonten, die einen Manager haben, schlägt fehl.	37088
Im Parameter `attributes` eines HTTP-`GET`-Requests werden die Namen von Eigenschaften, die in einer Überlagerungsdatei definiert sind, nicht RFC-konform formatiert.	37099
Fehler im RACF-Konnektor, wenn das RemoteConnectPlugin verwendet wird.	37103
Fehler in der Bildungsregel für `OLGUser.status`.	37138
SAP Schemaerweiterungen mit geschachtelten Where-Klauseln in der Tabellendefinition liefern nicht die erwarteten Datensätze.	37146
Die Darstellung der Protokollinformationen aus der Datenbank im Systemprotokoll erfolgt nicht in der richtigen Reihenfolge.	37155
Beliebige Änderungen an der Definition der Spalte `SAPComSMTP.SMTPAddr` führen zu einer Fehlermeldung.	37169

Gelöstes Problem	Fehler ID
Der Konsistenzcheck **DialogTable without Layout information** listet für alle kundenspezifischen Tabellen fehlende Darstellungsinformationen auf.	37181

Tabelle 11: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Die Bildungsregel für die Spalte Standard-E-Mail-Adresse von Identitäten (`Person.DefaultEmailAddress`) bildet keine Werte, wenn weder das Microsoft Exchange Modul noch das Domino Modul installiert sind und aktiv sind.	34915
Wenn eine Person in mehreren Entscheidungsschritten auf der selben Entscheidungsebene entscheidungsberechtigt ist, wird eine positive Entscheidung nicht übernommen, obwohl der Konfigurationsparameter **QER | ... | ReuseDecision** aktiviert ist.	35517
Basisobjekte für Ereignisse an `PersonWantsOrg` und `AttestationCase` sind nicht korrekt.	36430
Das Stammdatenformular für Identitäten konnte aufgrund eines externen Fehlers das automatisch Ausblenden einiger Oberflächenelemente im Manager verhindern.	36485
Beim Verschieben eines Produktes in ein anderes Regal werden Verlängerungsbestellungen nicht zurückgesetzt.	36634
In einigen Fällen kann es zu einem Fehler beim Transport von Entscheidungsworkflows kommen. Fehlermeldung: `PWODecisionStep: Write permission denied for value "CountApprover".`	36641
Produkteigentümer für Exchange Online Verteilergruppen werden nicht aus der Anwendungsrolle entfernt.	36668
Fehlende Sichtbarkeitsberechtigungen für **VI_4_ALLUSER_LOOKUP** für Azure Active Directory Dienstprinzipale zur Bestellung von Rollenberechtigungen.	36710
Im Manager kann das Datum für die Anlage von Benutzerkonten (`Person.TechnicalEntryDate`) nicht auf das Eintrittsdatum einer Person (`Person.EntryDate`) gesetzt werden.	36758
Fehlende Berechtigungen für Produkteigner **vi_4_ITSHOPADMIN_OWNER** für diverse Tabellen.	36777
Im Manager können in der Ergebnisliste für inaktive Identitäten keine Identitäten gelöscht oder eingefügt werden.	36784
Die Hilfstabelle für Bestellvorgänge (`PWOHelperPWO`) enthält sporadisch doppelte Einträge.	36805

Gelöstes Problem	Fehler ID
Fehlende Performance bei einigen DBQueue Prozessor-Aufträgen.	36826
Auf dem Überblicksformular für eine SAP Sammelrolle, wird der Zustand einer als ausstehend gekennzeichneten, zugewiesenen Einzelrolle nicht korrekt angezeigt.	36833
Wenn für eine Unternehmensrichtlinie keine Ausnahmegenehmigung zulässig ist, werden bei der Berechnung der Richtlinienverletzungen die Eigenschaften **Geprüft** (`IsDecisionMade`), **Entscheidung am** (`DecisionDate`) und die Begründung (`DecisionReason`) nicht mehr automatisch gesetzt.	36921
Wenn bei der Bestellung von Produkten mit einem Gültigkeitszeitraum (**Max. Tage gültig**) ein Gültig-bis-Datum angegeben wird, das kleiner als der Gültigkeitszeitraum ist, wird das Gültig-bis-Datum automatisch auf den Gültigkeitszeitraum erweitert.	36923, 431172
Das Skript `VI_MassDeleteDelegate` schlägt mit einer Fehlermeldung fehl, wenn sich eine der Bestellungen im Status **Abgebrochen** (Aborted) befindet.	36924
Fehler in der Prozedur `QER_PSlotResetOnInvalidRoot`.	36955
Sporadischer Fehler im Prozess `Created by QBMDBQueueProcess: handle object update for object type ITShopOrg`. Nach Reaktivierung läuft der Prozess fehlerfrei.	36965
Wenn eine Proxyview attestiert wird, beispielsweise Mitgliedschaften in Systemberechtigungen (`UNSAccountInUNSGroup`), und am Attestierungsverfahren der Inhalt des Snapshots auf **Objektreferenzen: nur Objektbeziehung 1-3** eingeschränkt ist, dann enthält der Snapshot im Attestierungsvorgang lediglich das Proxyobjekt (`UNSAccount`). Weitere Eigenschaften des zugehörigen Basisobjekts (beispielsweise `AADUser`) werden nicht angezeigt.	37035
Wenn der Konfigurationsparameter **QER | Attestation | ReuseDecision** aktiviert ist, wird eine positive Entscheidung aus einem vorherigen Entscheidungsschritt nicht übernommen, wenn ein dazwischenliegender Entscheidungsschritt negativ entschieden wurde.	37051
Die Complianceprüfung im Einkaufswagen verursacht für eine Subidentität eine falsch-positive Regelverletzung.	37079
Beim Einfügen von Identitäten werden auch dann Berechnungsaufträge für die Complianceprüfung eingestellt, wenn die Regelbedingung für alle Identitäten gilt.	37097
Fehler beim Importieren von aktivierten Unternehmensrichtlinien mit dem Database Transporter. Fehlermeldung: `QERPolicy: Write permission denied for value`	37098

Gelöstes Problem	Fehler ID
"IsWorkingCopy"	
Bei der Berechnung des Risikoindex für ein Objekt wird als **Geändert von** (XUserUpdated) **#** eingetragen.	37130
Falsche Sortierreihenfolge im Bericht **Bestellhistorie** im Manager.	37135
Fehler im Formatierungsskript für AOBApplication.NextRunDate bei der Ermittlung gültiger Datumswerte.	37150, 431402
Tippfehler in der deutschen Version der Mailvorlage **IT Shop Bestellung - Ablauf**.	37221

Siehe auch:

- Schemaänderungen auf Seite 54
- Patches für Synchronisationsprojekte auf Seite 63

Bekannte Probleme

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

Tabelle 12: Allgemein

Bekanntes Problem	Fehler ID
Fehler im Report Editor, wenn im Bericht Spalten verwendet werden, die im Report Editor als Schlüsselworte definiert sind. Workaround: Erstellen Sie Datenabfragen als SQL-Abfragen und nutzen Sie für die betroffenen Spalten Aliasnamen.	23521
Wird der Web Installer gleichzeitig in mehreren Instanzen gestartet, kann es zu Zugriffsfehlern kommen.	24198
Header-Zeilen in als CSV gespeicherten Reporten enthalten keine sprechenden Namen.	24657
Im Configuration Wizard können unzulässige Modulkombinationen ausgewählt werden. Dies führt erst bei Beginn der Schemainstallation zu Fehlern. Ursache: Der Configuration Wizard wurde direkt gestartet. Lösung: Verwenden Sie zur Installation der One Identity Manager Komponenten immer die autorun.exe. Damit ist sichergestellt, das keine unzulässigen Modulkombinationen ausgewählt werden.	25315

Bekanntes Problem	Fehler ID
Fehler bei der Verbindung über einen Anwendungsserver, wenn der private Schlüssel des Zertifikates, mit dem die `VI.DB` ihre Session-Information zu verschlüsseln versucht, nicht exportiert werden kann und der private Schlüssel damit der `VI.DB` nicht zur Verfügung steht. Lösung: Markieren Sie den privaten Schlüssel beim Export und Import des Zertifikats als exportierbar.	27793
Fehler beim Auslösen von Ereignissen auf eine View , welche keine UID-Spalte als Primärschlüssel besitzt. Primärschlüssel für Objekte im One Identity Manager bestehen immer aus einer oder, bei M:N-Tabellen, zwei UID-Spalten. Dies ist eine Basisfunktionalität im System. Die Definition einer View, die als Primärschlüssel den `XObjectKey` 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
In einem Bericht werden Variablen verwendet und für diese Variablen sind im Report Editor kundenspezifische Übersetzungen erfasst. Im generierten Bericht werden die Variablen jedoch nicht übersetzt. Ursache: Übersetzungen von Standardvariablen, die im Wörterbuch des Reportdesigners unterhalb der Kategorie **Quest** angezeigt werden, werden beim Generieren von Berichten mit den Werten aus der One Identity Manager-Datenbank überschrieben. Lösung: Legen Sie eigene Variablen an, die im Wörterbuch des Reportdesigners außerhalb der Kategorie **Quest** angeordnet sind. Diese Variablen können übersetzt werden.	36686
Die Konsistenzprüfung **Columns of type varchar(38) not PK and not FK.** erkennt Verstöße für Spalten mit einer Länge von `varchar(38)`, die	37072

Bekanntes Problem	Fehler ID
nicht als UID-Spalten gekennzeichnet sind. Lösung: Wählen Sie bei der Schemerweiterung eine andere Spaltenlänge. Entsprechend der Modellierungsrichtlinien sind Spalten mit einer Länge von `varchar(38)` reserviert für Spalten, die eine UID abbilden.	

Tabelle 13: Webanwendungen

Bekanntes Problem	Fehler ID
Bei der Installation des Web Portals mit dem Web Installer kann folgende Fehlermeldung auftreten: `Diese Zugriffssteuerungsliste liegt nicht in der kanonischen Form vor und kann aus diesem Grund nicht geändert werden.` Der Fehler tritt oft nach einem Windows 10 Anniversary Update auf. Lösung: Ändern Sie auf dem Elternordner der Webanwendung (standardmäßig `C:\inetpub\wwwroot`) die Berechtigungen für den Benutzer und wenden Sie diese Änderung an. Nehmen Sie anschließend diese Änderung wieder zurück.	26739
Die Bestelleigenschaften eines Produktes werden bei der Verlängerung oder Abbestellung im Web Portal nicht aus der ursprünglichen Bestellung in den Warenkorb übernommen. Ursache: Bestelleigenschaften können in unterschiedlichen, 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

Bekanntes Problem	Fehler ID

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

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 14: 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.	25401

Bekanntes Problem	Fehler ID
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`.	
Beim Anlegen von Microsoft Exchange Postfächern werden gegebenenfalls vorhandene sekundäre SIP-Adressen in primäre SIP-Adressen umgewandelt, sofern bisher keine primären SIP-Adressen hinterlegt waren.	27042
Fehler im Domino-Konnektor (`Error getting revision of schema type ((Server))`). Wahrscheinliche Ursache: Die HCL Domino-Umgebung wurde neu aufgebaut oder es wurden zahlreiche Einträge in das Domino-Verzeichnis eingefügt. Lösung: Aktualisieren Sie in der HCL Domino-Umgebung die Indexe im Domino-Verzeichnis manuell.	27126
Der SAP-Konnektor stellt keine Schemaeigenschaft bereit, um zu erkennen, ob ein Benutzer in der SAP R/3-Umgebung ein produktives Kennwort hat. Wenn diese Information im One Identity Manager zur Verfügung stehen soll, erweitern Sie das Schema und die Synchronisationskonfiguration. • Legen Sie eine kundenspezifische Spalte an der Tabelle `SAPUser` an. • Erweitern Sie im Synchronisationsprojekt das SAP Schema um einen neuen Schematyp, der die benötigte Information liefert. • Passen Sie die Synchronisationskonfiguration an.	27359
Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer 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.	29556

Bekanntes Problem	Fehler ID
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.	
Der Zielsystemabgleich zeigt in der Manager Webanwendung keine Informationen an. Workaround: Nutzen Sie den Manager, um den Zielsystemabgleich durchzuführen.	30271
Bei Bestellung eines Zugriffs auf ein Asset aus dem Bereich einer Zugriffsanforderungsrichtlinie, die für assetbasierten Sitzungszugriff vom Typ **Benutzer angegeben** konfiguriert ist, tritt im One Identity Safeguard folgender Fehler auf: `400: Bad Request -- 60639: A valid account must be identified in the request.` Die Bestellung wird im One Identity Manager abgelehnt und der Fehler in der Bestellung als Begründung angezeigt.	796028, 30963
Bei Inkonsistenzen in der SharePoint-Umgebung kann es passieren, dass bereits der Zugriff auf eine Eigenschaft einen Fehler verursacht. Der Fehler erscheint auch dann, wenn das Mapping der betroffenen Schemaeigenschaft deaktiviert wird. Ursache: Der SharePoint Konnektor lädt standardmäßig alle Objekteigenschaften in einen Cache. Lösung: • Korrigieren Sie den Fehler im Zielsystem. - ODER - • Deaktivieren Sie den Cache in der Datei `VI.Projector.SharePoint.<Version>.Host.exe.config`.	31017
Wenn eine SharePoint Websitesammlung 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. Voraus-	32149

Bekanntes Problem	Fehler ID

setzung dafür ist, dass auf dem Synchronisationsserver der SAP .Net Connector for .NET 4.0 on x64, mindestens Version 3.0.15.0 installiert ist.
WICHTIG: Da mit diesem Workaround die Datumsprüfung komplett umgangen wird, sollte er nur genutzt werden, wenn keine andere Lösung umsetzbar ist.
Um die Typkonvertierung zu deaktivieren, fügen Sie folgende Einstellungen in die Datei `StdioProcessor.exe.config` ein.
• In die vorhandene Sektion `<configSections>`:
`<sectionGroup name="SAP.Middleware.Connector">`
`<section name="GeneralSettings" type="SAP.Middleware.Connector.RfcGeneralConfiguration, sapnco, Version=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c7f7d23" />`
`</sectionGroup>`
• Eine neue Sektion:
`<SAP.Middleware.Connector>`
`<GeneralSettings anyDateTimeValueAllowed="true" />`
`</SAP.Middleware.Connector>`	

Die in der Prozesskomponente `PowershellComponentNet4` im Parameter `OutputFile` zu erzeugende Datei enthält keine Fehlermeldungen. 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	33104

Bekanntes Problem	Fehler ID
anderes Google Workspace Benutzerkonto übertragen. Der Transfer scheitert an den Nutzerdaten der Applikation Rocket. Workaround: Hinterlegen Sie in den erweiterten Einstellungen der Systemverbindung zu Google Workspace ein Nutzerdatentransfer XML. In diesem XML-Dokument schränken Sie die Liste der zu übertragenden Nutzerdaten ein. Führen Sie nur die Google Applikationen auf, deren Nutzerdaten Sie weiterhin benötigen. Ausführliche Informationen und ein Beispiel-XML finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Google Workspace-Umgebung*.	
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.	34903
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
Nach einer Aktualisierung von One Identity Manager Version 8.0 oder Version 8.1 auf One Identity Manager Version 8.2.1 oder höher, kann es vorkommen, dass PowerShell-Skripte, die auf das Az-PowerShell-Modul (`Import-Module Az`) verweisen, nicht funktionieren. In einer PowerShell, die auf demselben Host gestartet wird, funktionieren die Skripte ohne Fehler. Bei der Ausführung der Prozessfunktion `ExecuteScript` durch die Prozesskomponente `PowerShellComponentNet4` werden Fehlermeldungen protokolliert.	37116

Bekanntes Problem	Fehler ID

Beispiel:
`Entry point was not found.`
Ursache:
Mit One Identity Manager Version 8.2.1 oder höher wird eine Bibliothek `Azure.Core.dll` mit einer bestimmten Version mitgeliefert. Das kundenspezifische PowerShell-Skript hängt möglicherweise von einer neueren Version des Az-PowerShell-Moduls ab. Wenn der One Identity Manager Service das Skript ausführt, wird die lokal gespeicherte `Azure.Core.dll`verwendet, wodurch die Abhängigkeit unterbrochen wird.
Mögliche Workarounds: Prüfen Sie die Einsatzmöglichkeit der folgenden Workarounds hinsichtlich Eingabeparameter und Rückgabewert.
• Rufen Sie PowerShell als Unterprozess auf
Um einen PowerShell-Befehl aus dem aktuellen Prozess heraus auszuführen, starten Sie einen neuen PowerShell-Prozess direkt mit dem Befehlsaufruf.
`pwsh -c 'Invoke-ConflictingCommand'`
• Verwenden Sie die Prozesskomponente `CommandComponent` mit der Prozessfunktion `Execute`, um die PowerShell-Anwendung mit folgendem Befehlsaufruf zu starten.
`powershell -c 'Invoke-ConflictingCommand'`	

Tabelle 15: Identity Management und Access Governance

Bekanntes Problem	Fehler ID
Bei der Genehmigung einer Bestellung mit Selbstbedienung wird das Ereignis `Granted` für den Entscheidungsschritt nicht ausgelöst. In kundenspezifischen Prozessen kann stattdessen das Ereignis `OrderGranted` genutzt werden.	31997
Wenn eine Zuweisung über die Rollenhierarchie vererbt wird, wird an der geerbten Zuweisung das **Bit 1** gesetzt. Geerbte Zuweisungen sind folglich immer indirekt zugewiesen, auch wenn sie ursprünglich direkt, über eine dynamische Rolle oder eine Zuweisungsbestellung entstanden sind.	35193
Wenn an einer Leistungsposition **Max. Tage gültig** verkleinert wird, so dass genehmigte Bestellungen damit bereits abgelaufen sind, dann können diese Bestellungen nicht mehr abbestellt werden. Lösung: Erstellen Sie einen Prozess für das Basisobjekt `AccProduct`, der bei Änderungen an `AccProduct.MaxValidDays` ausgelöst wird. Der Prozess berechnet das Gültig-bis-Datum für diese Bestellungen (`PersonWantsOrg.ValidUntil`)	36349

Bekanntes Problem	Fehler ID
aus `PersonWantsOrg.ValidFrom` und `AccProduct.MaxValidDays`. Danach können diese Bestellungen abbestellt werden.	

Tabelle 16: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
Die Installation des One Identity Manager Service mit Server Installer auf einem Windows Server funktioniert nicht, wenn die Einstellung **File and Printer Sharing** am Server deaktiviert ist. Auf einem Domänen-Controller ist diese Einstellung aus Sicherheitsgründen deaktiviert.	24784
Beim Verbinden mit einer Oracle Database kommt es sporadisch zu einem der folgenden Fehler: TNS-12516, TNS-12519 oder ORA-12520. Erneute Verbindungsversuche sind jedoch meist erfolgreich. Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am Server konfigurierte Limit.	27830
In einem mehrseitigen Synchronisationsprotokoll kann nicht mit der Maus und mit den Pfeiltasten navigiert werden. Ursache: Die StimulReport.Net-Komponente der Firma Stimulsoft behandelt den Bericht als eine Seite.	29051
Gültiger CSS-Code verursacht einen Fehler unter Mono, wenn doppelte Schlüssel vorhanden sind. Weitere Informationen finden Sie unter https://github.com/mono/mono/issues/7455.	762534, 762548, 29607
Mitgliedschaften in Active Directory Gruppen vom Typ **Universal** in einer untergeordneten Domäne werden im Zielsystem nicht entfernt, wenn eines der folgenden Windows Updates installiert ist: • Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 One Identity 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`-	31998

Bekanntes Problem	Fehler ID
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 in One Identity 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 9.1.1 zu Version 9.2.

Konfigurationsmodul

- Neue Spalte `DialogParameter.QueryDisplayType` für die Darstellung von Daten zu Werteabfragen.
- Neue Spalte `DialogTable.IsApiServerEnabled` (in Vorbereitung für zukünftige Funktionen).
- Neue Spalten `DialogTree.InitScript` und `DialogTree.ListTitle` zur kontextabhängigen Darstellung von Anzeigetexten in der Benutzeroberfläche.

- Neue Spalte `QBMHtmlApp.UID_QBMDBPrincipal` zur Abbildung der minimalen Berechtigungsebene für die Nutzung der HTML-Anwendungen.
- Neue Spalte `DialogDeferredOperation.XObjectKey`.
- Neue Spalten `QBMNonLinearDepend.XUserInserted`, `QBMNonLinearDepend.XUserUpdated`, `QBMNonLinearDepend.XDateInserted` und `QBMNonLinearDepend.XDateUpdated`.
- Neue Tabellen `QBMConfigLibrary` und `QBMConfigLibraryCategory` zur Bereitstellung einer Konfigurationsbibliothek für Bildungsregeln und Formatierungsregeln.
- Neue Tabelle `QBMMissingDisplayRight` zur schnelleren Ermittlung von Anzeigeberechtigungen.
- Neue Tabelle `QBMUserConfig` zur internen Abbildung von Benutzereinstellungen.

Modul Zielsystemsynchronisation

- Neue Spalte `DPRProjectionConfig.GeneralConcurrenceStrategy` zur Festlegung einer Strategie zur Kollisionserkennung.
- Neue Spalten `DPRProjectionStartInfo.FailureHandlingMode` und `DPRProjectionStartInfo.FailureHandlingRetryCycles` zur verbesserten Behandlung von fehlgeschlagenen Objekten.
- Neue Spalten `DPRProjectionStartInfo.SysConcurrenceCacheLifeTime` und `DPRProjectionStartInfo.SysConcurrenceCheckMode` zur verbesserten Erkennung von Verarbeitungskonflikten.
- Neue Spalten `DPRSchemaProperty.IsMvpOrderSignificant` und `DPRSystemMappingRule.MvpOrderBehavior` zur Behandlung von MVP-Werten bei der Erkennung unzulässiger Änderungen.

Zielsystem Basismodul

- Neue Spalten `TSBVAccountTable.ColumnNameAccDisabled` und `TSBVAccountTable.IsPersonAuto4Disabled` zur besseren Abbildung von Benutzerkonten für gesperrte Identitäten.
- Die Spalten `TSBVUNSDomain.AlternatePropertyCaptions`, `TSBVUNSRoot.AlternatePropertyCaptions` und `UNSRoot.AlternatePropertyCaptions` wurde gelöscht.

Azure Active Directory Modul

- Neue Spalte `AADAdministrativeUnit.UID_AERoleOwner` zur Abbildung von Eigentümern für Verwaltungseinheiten.
- Neue Spalte `AADApplication.UID_AERoleOwner` zur Abbildung von Eigentümern für Anwendungen.
- Neue Spalte `AADServicePrincipal.UID_AERoleOwner` zur Abbildung von Eigentümern für Dienstprinzipale.

- Neue Spalten zur Unterstützung weiterer Identity Management-relevanter Eigenschaften für Benutzerkonten.
  - AADUser.EmployeeHireDate
  - AADUser.EmployeeLeaveDateTime
  - AADUser.EmployeeType
  - AADUser.EodCostCenter
  - AADUser.EodDivision
- Neue Spalten zur Ermittlung von Anmeldezeiten für Benutzerkonten.
  - AADUser.siaLastNISignInDateTime
  - AADUser.siaLastNISignInRequestId
  - AADUser.siaLastSignInDateTime
  - AADUser.siaLastSignInRequestId
- Neue Spalte AADOrganization.RoleBehavior zur Abbildung des Azure Active Directory Rollenmanagements.
- Neue Tabellen zur Abbildung des Azure Active Directory Rollenmanagements.
  - AADBaseTreeHasScopedRLAsgn
  - AADBaseTreeHasScopedRLElgb
  - AADGroupInScopedRLAsgn
  - AADGroupInScopedRLElgb
  - AADPrincipalInScopedRLAsgn
  - AADPrincipalInScopedRLElgb
  - AADRole
  - AADRoleAssignment
  - AADRoleEligibility
  - AADRoleManagementPolicy
  - AADScopedRLAsgn
  - AADScopedRLElgb
  - AADUserInScopedRLAsgn
  - AADUserInScopedRLElgb
  - DepartmentHasScopedRLAsgn
  - DepartmentHasScopedRLElgb
  - LocalityHasScopedRLAsgn
  - LocalityHasScopedRLElgb
  - OrgHasScopedRLAsgn
  - OrgHasScopedRLElgb

- ProfitCenterHasScopedRLAsgn
- ProfitCenterHasScopedRLElgb

Exchange Online Modul

- Neue Spalten zur Abbildung hierarchischer Adressbücher.
  - AADOrganization.UID_O3EDLHABRoot
  - O3EDL.IsHierarchicalGroup
  - O3EDL.PhoneticDisplayName
  - O3EDL.SeniorityIndex
  - O3EMailbox.PhoneticDisplayName
  - O3EMailbox.SeniorityIndex

Microsoft Teams Modul

- Neue Spalte O3TTeam.tmsAllowCreatePrivateChannels zur Angabe ob, ob Mitglieder private Kanäle erstellen oder aktualisieren können.
- Neue Tabelle O3TTeamTemplate und neue Spalte O3TTeam.UID_O3TTeamTemplate zur Abbildung von Teamvorlagen.

Active Directory Modul

- Neue Spalten zur Unterstützung von POSIX-Eigenschaften für Benutzerkonten, Kontakte und Gruppen.
  - ADSAccount.Gecos
  - ADSAccount.GidNumber
  - ADSAccount.LoginShell
  - ADSAccount.UidNumber
  - ADSAccount.UidPosix
  - ADSAccount.UnixHomeDirectory
  - ADSContact.Gecos
  - ADSContact.GidNumber
  - ADSContact.LoginShell
  - ADSContact.UidNumber
  - ADSContact.UidPosix
  - ADSContact.UnixHomeDirectory
  - ADSGroup.GidNumber

Microsoft Exchange Modul

- Neue Spalten zur Abbildung hierarchischer Adressbücher.
  - EX0DL.IsHierarchicalGroup
  - EX0DL.PhoneticDisplayName
  - EX0DL.SeniorityIndex
  - EX0MailBox.PhoneticDisplayName
  - EX0MailBox.SeniorityIndex
  - EX0MailContact.PhoneticDisplayName
  - EX0MailContact.SeniorityIndex
  - EX0MailUser.PhoneticDisplayName
  - EX0MailUser.SeniorityIndex
  - EX0Organization.UID_EX0DLHABRoot
- Neue Tabelle EX0VHABMembers zur Abbildung hierarchischer Adressbücher.
- Neue Tabelle EX0DLSendAsPerm zur Abbildung von Sendeberechtigungen für E-Mail-aktivierte Verteilergruppen.

Exchange Hybrid Modul

- Neue Spalten EXHRemoteMailbox.PhoneticDisplayName und EXHRemoteMailbox.SeniorityIndex zur Abbildung hierarchischer Adressbücher.

LDAP Modul

- Neue Spalten zur Unterstützung der eduPerson-Objektklasse.
  - LDAPAccount.EduPersonAffiliation
  - LDAPAccount.EduPersonAnalyticsTag
  - LDAPAccount.EduPersonAssurance
  - LDAPAccount.EduPersonEntitlement
  - LDAPAccount.EduPersonNickname
  - LDAPAccount.EduPersonOrcId
  - LDAPAccount.EduPersonOrgDN
  - LDAPAccount.EduPersonOrgUnitDN
  - LDAPAccount.EduPersonPrimaryAffiliation
  - LDAPAccount.EduPersonPrimaryOrgUnitDN
  - LDAPAccount.EduPersonPrincipalName
  - LDAPAccount.EduPersonPrincipalNamePrior
  - LDAPAccount.EduPersonScopedAffiliation

- LDAPAccount.EduPersonTargetedId
- LDAPAccount.EduPersonUniqueId

Domino Modul

- Neue Spalten zur Unterstützung des Roaming von Notes Benutzerkonten.
  - NDOUser.RoamAB
  - NDOUser.RoamCleanPer
  - NDOUser.RoamCleanSetting
  - NDOUser.RoamExtFiles
  - NDOUser.RoamingUser
  - NDOUser.RoamMode
  - NDOUser.RoamSubDir
  - NDOUser.UID_NDOServerRoamSrvr

OneLogin Modul

- Neue Spalte OLGUser.AccountDisabled zur Angabe, ob das Benutzerkonto gesperrt ist.

Privileged Account Governance Modul

- Neue Tabellen PAGPartition und PAGPartitionIsManagedBy zur Abbildung von Partitionen.
- Neue Spalten PAGAsset.UID_PAGPartition und PAGDirectory.UID_PAGPartition zur Abbildung von Partitionen.
- Neue Spalten zur Unterstützung von Zugriffsanforderungen für API-Schlüssel.
  - PAGAstAccount.AllowApiKeyRequest
  - PAGAstAccount.HasApiKeys
  - PAGAstAccount.HasTotpAuthenticator
  - PAGAstAccount.IsApplicationAccount
  - PAGUserAttestation.AllowApiKeyRequest
- Neue Spalte PAGReqPolicy.LinkedAccountScopeFiltering und PAGReqPolicy.UseAltLoginName für PAM Zugriffsanforderungsrichtlinien.
- Neue Spalte PAGEntl.XDateSubItem zur Abbildung des Änderungsdatums abhängiger Objekte.
- Neue Tabelle PAGAuditLog zur Abbildung von Prüfprotokollen zur Unterstützung von Behavior Driven Governance.

Modul Unix-basierte Zielsysteme

- Neue Spalten zur Abbildung von Anmeldeinformationen für Benutzerkonten.
  - UNXAccount.LastLogin
  - UNXAccount.LastLoginString
  - UNXAccount.LastPasswordChange
  - UNXHost.UID_DialogTimeZone

Identity Management Basismodul

- Neue Spalte Person.LeaveOfAbsenceReason als Grund der Abwesenheit einer Identität.
- Neue Spalte QERTermsOfUse.IsAcceptRequiresMfa zur Angabe, ob zum Akzeptieren der Nutzungsbedingung eine Multifaktor-Authentifizierung erforderlich ist.

Modul Unternehmensrichtlinien

- Neue Spalten QERPolicy.IsToAttestImmediately und QERPolicy.ObjectKeyAttPolicy für die Unterstützung der automatischen Attestierung von Richtlinienverletzungen.

Modul Attestierung

- Neue Spalte AttestationPolicy.IsNoRunOnEmptyResult zur Angabe, ob ein leerer Attestierungslauf generiert werden soll, wenn kein zu attestierendes Objekt ermittelt wird.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 9.1.1 zu Version 9.2. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 90.

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 63.

Tabelle 17: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Modul Zielsystemsynchronisation	Automatic One Identity Manager Synchronization	geändert
Azure Active Directory Modul	Azure Active Directory Synchronization	geändert
	Azure Active Directory B2C tenant	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	keine
	Oracle E-Business Suite CRM data	keine
	Oracle E-Business Suite HR data	keine
	Oracle E-Business Suite OIM data	keine
Microsoft Exchange Modul	Microsoft Exchange 2013/2016/2019 Synchronization (v2)	geändert
Google Workspace Modul	Google Workspace Synchronization	keine
LDAP Modul	AD LDS Synchronization	keine
	AD LDS Synchronization (version 2)	keine
	OpenDJ Synchronization	keine
	OpenDJ Synchronization (version 2)	keine
	Generic LDAP Synchronization (version 2)	keine
	Oracle DSEE Synchronization (version 2)	keine

Modul	Synchronisationsvorlage	Art der Änderung
Domino Modul	Lotus Domino Synchronization	geändert
Exchange Online Modul	Exchange Online Synchronization (v2)	keine
Microsoft Teams Modul	Microsoft Teams (via Azure Active Directory)	keine
OneLogin Modul	OneLogin Domain Synchro-nization	keine
Privileged Account Governance Modul	One Identity Safeguard Synchro-nization	geändert
SAP R/3 Benutzermanagement-Modul	SAP R/3 Synchronization (Base Administration)	geändert
	SAP R/3 (CUA subsystem)	keine
Modul SAP R/3 Analyseberechtigungen Add-on	SAP R/3 BW	keine
Modul SAP R/3 Compliance Add-on	SAP R/3 authorization objects	keine
Modul SAP R/3 Strukturelle Profile Add-on	SAP R/3 HCM authentication objects	keine
	SAP R/3 HCM employee objects	keine
SharePoint Modul	SharePoint Synchronization	keine
SharePoint Online Modul	SharePoint Online Synchro-nization	keine
Modul Universal Cloud Interface	SCIM Connect via One Identity Starling Connect	geändert
	SCIM Synchronization	geändert
	SCIM Synchronisation einer SAP Cloud ALM Anwendung	neu
Modul Unix-basierte Zielsysteme	Unix Account Management	geändert
	AIX Account Management	geändert

Patches für Synchronisationsprojekte

Im One Identity Manager 9.2 werden Patches für folgende Patchtypen bereitgestellt:

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

Um bestehende Synchronisationsprojekte an die One Identity Manager Version 9.2 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 9.2 kompatibel.

Patches für neue Funktionen können optional angewendet werden.

Nachfolgend finden Sie eine Liste der Patches für Synchronisationsprojekte, die im One Identity Manager 9.2 neu bereitgestellt werden. Es sind nur die Patches aufgelistet, die nach der Version 9.1.1 neu erstellt wurden. Einen Überblick über die Patches früherer One Identity Manager Versionen erhalten Sie in den jeweiligen Versionsinformationen für diese Versionen.

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

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

Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 90.

Tabelle 18: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36755	Deaktivierung des Synchronisationspuffers für die Zentraldatenbank	Deaktiviert den Synchronisationspuffer für verschiedene virtuelle Schemaeigenschaften im Schema der Zentraldatenbank in Synchronisationsprojekten für die Systemsynchronisation.	36755
	Meilenstein 9.2	Meilenstein für den Kontext **DPR**.	
	Meilenstein 9.2	Meilenstein für den Kontext **One Identity Manager**.	

Tabelle 19: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36596	Unterstützung von Verbindungszertifikaten	Legt die Variable `CP_CertificateThumbprint` im Standardvariablenset an. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36596
VPR#36729	Neue Schemaeigenschaften für Azure Active Directory Benutzerkonten	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `employeeHireDate`, `employeeLeaveDateTime`, `employeeType`, `eoddivision` and `eodcostcenter` in das Mapping `User` ein. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36729
VPR#36799	Setzt Filter in Mehrfachreferenzregeln	Fügt Mitgliederfilter in verschiedene Mehrfachreferenzregeln für die Schemaeigenschaft `Owners` ein. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36799
VPR#33776	Neue Schemaeigenschaften zur Abbildung des Anmeldezeitpunkts von Azure Active Directory Benutzerkonten	Fügt Property-Mapping-Regeln für die Abbildung des letzten Anmeldezeitpunkts von Benutzerkonten (`siaLastNISignInDateTime`, `siaLastNISignInRequestId`, `siaLastSignInDateTime`, `siaLastSignInRequestId`) in das Mapping `User` ein. Auf diese Schemaeigenschaften kann nur zugegriffen werden, wenn eine Azure Active Directory-Premium-Lizenz vorhanden ist.	33776

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35769	Ermöglicht die Abbildung von Dienstprinzipalen als Eigentümer von Dienst-prinzipalen	Erweitert den Mitgliederfilter der Property-Matching-Regel `vrtOwners_Owners` im Mapping `ServicePrincipal` auf Dienst-prinzipale. Dieser Patch wird während der Aktualisierung von One Identity Manager automa-tisch angewendet.	35769
VPR#35513	Unterstützung von RBAC und PIM Funktionen	Erweitert die Synchro-nisationskonfiguration für die Synchronisation von Objekte für die rollenbasierte Zugriffs-steuerung (RBAC) und das Privi-leged Identity Management (PIM). Dieser Patch wird während der Aktualisierung von One Identity Manager automa-tisch angewendet.	35513
	Meilenstein 9.2	Meilenstein für den Kontext **Azure Active Directory**.	

Tabelle 20: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#14634	Neue Mappings zur Abbildung von POSIX-Eigenschaften	Fügt die Mappings `posixContact`, `posixGroup` und `posixUser` für die Abbildung von POSIX-Eigenschaften für Benutzerkonten, Gruppen und Kontakte ein.	14634
	Meilenstein 9.2	Meilenstein für den Kontext **Active Directory**.	

Tabelle 21: Patches für Active Roles

Patch ID	Patch	Beschreibung	Fehler ID
VPR#14634_ ARS	Neue Property-Mapping-Regeln zur Abbildung von POSIX-Eigen-schaften	Fügt neue Property-Mapping-Regeln in die Mappings `User`, `InetOrgPerson`, `Group` und `Contact` für die Abbildung von POSIX-Eigenschaften ein.	14634
	Meilenstein 9.2	Meilenstein für den Kontext **Active Roles**.	

Tabelle 22: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35776	Erweiterung der Senden-als-Berechtigungen	Erweitert die Synchronisationskonfiguration zur Unterstützung der Senden-als-Berechtigungen für Verteilergruppen. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	35776
VPR#35779	Neue Property-Mapping-Regeln zur Abbildung eines hierarchischen Adressbuchs	Fügt neue Property-Mapping-Regeln in verschiedene Mappings ein, um ein hierarchisches Adressbuch abzubilden. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	35779
	Meilenstein 9.2	Meilenstein für den Kontext **Microsoft Exchange**.	

Tabelle 23: Patches für HCL Domino

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36087	Mapping der Roaming-Eigenschaften von Benutzerkonten	Erweitert das Mapping `Person` zur Abbildung der Roaming-Eigenschaften von Benutzerkonten. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36087
VPR#36831	Entfernen von Quotas zum Löschen von Objekten	Entfernt Quotas für die Methode `Delete object` aus den Synchronisationsschritten `CertifierRequest` und `AdminRequest`.	36831
	Meilenstein 9.2	Meilenstein für den Kontext **HCL Domino**.	

Tabelle 24: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35780	Neue Property-Mapping-Regeln zur	Fügt neue Property-Mapping-Regeln in verschiedene Mappings	35780

Patch ID	Patch	Beschreibung	Fehler ID
	Abbildung eines hierarchischen Adressbuchs	ein, um ein hierarchisches Adressbuch abzubilden. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	
	Meilenstein 9.2	Meilenstein für den Kontext **Exchange Online**.	

Tabelle 25: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36961	Entfernen ungenutzter Schemaeigenschaften	Entfernt ungenutzte Schemaeigenschaften aus dem Schematyp `Web`.	36961
	Meilenstein 9.2	Meilenstein für den Kontext **SharePoint Online**.	

Tabelle 26: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36044	Unterstützung von One Identity Safeguard Partitionen	Erweitert die Synchronisationskonfiguration zur Unterstützung von One Identity Safeguard Partitionen.	36044
VPR#36315	Abbildung der One Identity Safeguard Prüfprotokolle	Erweitert die Synchronisationskonfiguration, um die One Identity Safeguard Prüfprotokolle (`AuditLog`) einzulesen.	36315
VPR#36617	Unterstützung für One Identity Safeguard 7.2 und 7.3	Erweitert die Synchronisationskonfiguration zur Unterstützung der Versionen 7.2 und 7.3 von One Identity Safeguard.	36617, 36943
	Meilenstein 9.2	Meilenstein für den Kontext **Privileged Account Management**.	

Tabelle 27: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36970	Nachladeschwellwert für Benutzerkonten setzen	Setzt den Nachladeschwellwert im Synchronisationsschritt `user` auf den Wert **4**.	36970
	Meilenstein 9.2	Meilenstein für den Kontext **SAP R/3**.	

Tabelle 28: Patches für SAP R/3 Berechtigungsobjekte

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35904	Entfernen ungenutzter Verarbeitungsmethoden	Entfernt ungenutzte Verarbeitungsmethoden (`Update`) in verschiedenen Synchronisationsschritten.	35904
	Meilenstein 9.2	Meilenstein für den Kontext **SAP R/3**.	

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

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36376	Neue Variable zur Konfiguration der Listeneinstellungen	Fügt eine Variable zur Konfiguration der Elemente pro Seite bei Anfragen für die Objektliste in das Standardvariablenset und die Verbindungsparameter ein. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36376
VPR#36985	Korrektur von Schemaerweiterungen	Speichert die Namen der Erweiterungen von Schematypen im Schema. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36985
	Meilenstein 9.2	Meilenstein für den Kontext **SCIM**.	

Tabelle 30: Patches für Unix

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36688	Neue Property-Mapping-Regeln zur Abbildung des letzten Anmeldedatums und der letzten Kennwortänderung von Benutzerkonten	Fügt Property-Mapping-Regeln für `LastPasswordChange` und `LastLogin` in das Mapping `User` ein. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36688
	Meilenstein 9.2	Meilenstein für den Kontext **Unix**.	

Abgekündigte Funktionen

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

- Folgende Skripte wurden entfernt.
  - VI_GetValueOfObject
  - VID_GetValueOfDialogObject
  - VI_ITDataFromOrg
  - VI_AE_ITDataFromOrg
  - VI_GetOrgUnitFromCertifier
  - VI_ConvertDNToCanonicalName
  - VI_PersonAuto_LDAP
  - VI_PersonAuto_ADS
  - VI_PersonAuto_EBS
  - VI_PersonAuto_Notes
  - VI_PersonAuto_SAP
  - VI_PersonAuto_SharePoint_SPSUser
  - VI_GetAttestationObject
  - VI_GetDNParser
  - TSB_Find_And_Use_Linked_Account_For_AccountDef

- Folgende Konfigurationsparameter wurden entfernt.
    - TargetSystem | ADS | DBDeleteOnError
    - TargetSystem | ADS | VerifyUpdates
    - TargetSystem | EBS | DBDeleteOnError
    - TargetSystem | NDO | VerifyUpdates
    - TargetSystem | SAPR3 | DBDeleteOnError
    - TargetSystem | SAPR3 | VerifyUpdates
    - TargetSystem | SharePoint | DBDeleteOnError

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

- Folgenden Funktionen werden für den One Identity Manager Service zukünftig nicht mehr unterstützt.
    - FileJobProvider
    - FileJobDestination
    - FileJobGate
    - FTPJobProvider
    - FTPJobDestination
    - HTTPJobProvider
    - HTTPJobDestination
    - HTTPJobGate
- Der Web Designer und die Web Designer-basierten Webanwendungen werden zukünftig nicht mehr unterstützt. Verwenden Sie die HTML-Webanwendungen, die über den API Server bereitgestellt werden.
- Die Tabelle `PersonPasswordHistory` wird in zukünftigen Versionen entfernt.
- Folgende Skripte sind als veraltet gekennzeichnet. Bei der Kompilierung wird eine entsprechende Warnung ausgegeben.
    - VI_AE_BuildCentralAccount
    - VI_AE_BuildCentralAccountGlobalUnique
    - VI_BuildInternalName
    - VI_AE_CreatedefaultMailAddress
    - VI_AE_BuildCentralSAPAccount

Systemanforderungen

Stellen Sie vor der Installation von One Identity Manager sicher, dass Ihr System den nachfolgenden minimalen Hardware- und Systemanforderungen genügt.

Für detaillierte Informationen zu den Systemvoraussetzungen lesen Sie das *One Identity Manager Installationshandbuch*.

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

Jede One Identity Manager Installation kann virtualisiert werden. Stellen Sie sicher, dass der jeweiligen One Identity Manager-Komponente die laut Systemanforderung spezifizierte Leistung und Ressourcen zur Verfügung stehen. Idealerweise sollten Ressourcenzuordnungen für den Datenbankserver statisch festgesetzt werden. Die Virtualisierung einer One Identity Manager Installation sollte von Experten mit einem fundierten Wissen über Virtualisierungstechniken vorgenommen werden.

Unterstützte Datenbanksysteme

One Identity Manager unterstützt folgende Datenbanksysteme:

- SQL Server
- Verwaltete Instanzen in Azure SQL-Datenbank
- Azure SQL-Datenbank
- Amazon RDS for SQL Server

Minimalanforderungen für den Einsatz von SQL Server als Datenbankserver

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

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung (nicht-produktiv) 16 physische Kerne mit 2.5 GHz+ Taktung (produktiv) HINWEIS: Aus Performancegründen wird der Einsatz von 16 physischen Kernen empfohlen.
Arbeitsspeicher	16 GB+ RAM (nicht-produktiv) 64 GB+ RAM (produktiv)
Freier	100 GB

Festplattenspeicher	
Betriebssystem	Windows Betriebssysteme • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. UNIX und Linux Betriebssysteme • Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.
Software	Unterstützt werden die Versionen: • SQL Server 2019 Standard Edition (64-Bit) mit aktuellem kumulativen Update • SQL Server 2022 Standard Edition (64-Bit) mit aktuellem kumulativen Update HINWEIS: Aus Performancegründen wird für produktive Systeme der Einsatz der SQL Server Enterprise Edition empfohlen. • Kompatibilitätsgrad für Datenbanken: SQL Server 2019 (150) • Standard-Sortierschema: Case-Insensitiv, SQL_Latin1_General_CP1_CI_AS (Empfehlung) • SQL Server Management Studio (empfohlen)

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

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

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

Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank

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

Minimalanforderungen für Clients

Auf den Clients sind die folgenden Systemvoraussetzungen zu gewährleisten.

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

Minimalanforderungen für Jobserver

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

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	16 GB RAM
Freier Festplat-	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 4.8 oder höher HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers. Linux Betriebssysteme • Mono 6.10 oder höher

Minimalanforderungen für Webserver

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

Prozessor	4 physische Kerne mit 1.65 GHz+Taktung
Arbeitsspeicher	4 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2

	• Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden. Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für Apache HTTP Server.

Zusätzliche Software	Windows Betriebssysteme
	• Microsoft .NET Framework Version 4.8 oder höher
	• Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.8 und den Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions
	  • Web Server > Application Development > ISAPI Filters
	  • Web Server > Security > Basic Authentication
	  • Web Server > Security > Windows Authentication
	  • Web Server > Performance > Static Content Compression
	  • Web Server > Performance > Dynamic Content Compression
	Linux Betriebssysteme
	• NTP - Client
	• Mono 6.10 oder höher
	• Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
	  • mod_mono
	  • rewrite
	  • ssl (optional)

Minimalanforderungen für Anwendungsserver

Zur Installation des Anwendungsservers sind die folgenden Systemvoraussetzungen zu gewährleisten.

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

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

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

Linux Betriebssysteme

- NTP - Client
- Mono 6.10 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 31: Unterstützte Datensysteme

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

Konnektor	Unterstützte Datensysteme
	Information Models) zu gewährleisten. HINWEIS: Abhängig vom Schema können weitere Anpassungen bezüglich des Schemas und der Provisionierungsprozesse erforderlich sein.
Web Service Konnektor	Beliebige SOAP Web Services, die eine wsdl zur Verfügung stellen. HINWEIS: Es kann der Web Service Assistent, benutzt werden, um die Konfiguration für das Schreiben der Daten zum Web Service zu generieren. Für das Lesen und Synchronisieren der Daten sind zusätzliche Skripte erforderlich, welche die Methoden des Web Service Konnektors nutzen.
Active Directory Konnektor	Active Directory, welches mit Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 und Windows Server 2022 ausgeliefert wird.
Microsoft Exchange Konnektor	• Microsoft Exchange 2013 mit kumulativem Update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 mit kumulativem Update 1 • MicrosoftExchange Hybrid-Umgebungen
SharePoint Konnektor	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
SAP R/3 Konnektor	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55, 7.56 und 7.69 • SAP ECC 5.0 und 6.0 • SAP S/4HANA On-Premise-Edition 1.0 und 2.0 ab SAP BASIS 7.40 SR 2 und 7.50 (auch für Installationen mit SAP BASIS 7.53)
Unix Konnektor	Unterstützt werden die gängigsten Unix und Linux Derivate. Weitere Informationen finden Sie in den Spezifikationen für One Identity Authentication Services.
Domino Konnektor	• IBM Domino Server Version 8, 9 und 10 • HCL Domino Server Version 11 und 12

Konnektor	Unterstützte Datensysteme
	• IBM Notes Client 8.5.3 und 10.0 • HCL Notes Client Version 11.0.1 und 12.0 Die 64-Bit-Variante des Notes Client 12.0.1 wird derzeit nicht unterstützt. Für HCL Domino Server und HCL Notes Client wird die selbe Hauptversion eingesetzt.
Generischer Datenbankkonnektor	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe Konnektoren	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell Konnektor	• Windows PowerShell Version 3 oder höher
Active Roles Konnektor	• Active Roles 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.5, 7.5.2, 7.5.3, 7.6, 8.0, 8.1.1 und 8.1.3
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.

Konnektor	Unterstützte Datensysteme
	• 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: Protocol) sind zu gewährleisten.
Exchange Online Konnektor	• Microsoft Exchange Online
Google Workspace Konnektor	• Google Workspace
Oracle E-Business Suite Konnektor	• Oracle E-Business Suite Version 12.1, 12.2 und 12.2.10
SharePoint Online Konnektor	• Microsoft SharePoint Online
One Identity Safeguard Konnektor	• One Identity Safeguard Version 6.0, 6.7, 6.13, 7.0, 7.1, 7.2 und 7.3 Für die im einzelnen unterstützten Versionen finden Sie auf dem One Identity Manager Installationsmedium im Verzeichnis `Modules\PAG\dvd\AddOn\safeguard-ps` das passende Windows PowerShell Modul. Versionen, für die kein Windows PowerShell Modul auf dem One Identity Manager Installationsmedium vorhanden ist, werden nicht unterstützt.

Long Term Support (LTS) und Feature Releases

Sie haben die Wahl zwischen zwei Wegen, um Releases zu erhalten; Long Term Support (LTS) Release oder Feature Release.

Long Term Support (LTS)

- Die erste One Identity Manager LTS-Version ist 9.0. Bei allen LTS-Versionen von One Identity Manager bezeichnet die erste Ziffer die Version und die zweite Ziffer ist immer eine Null (zum Beispiel 9.0).
- Maintenance LTS Releases (auch kumulative Updates): Es wird eine dritte Ziffer hinzugefügt, zum Beispiel 9.0.1.

Feature Releases

- Die Versionsnummern der Feature Releases sind zweistellig (zum Beispiel 9.1, 9.2 und so weiter).

Die folgende Tabelle zeigt einen Vergleich von Long Term Support (LTS) Release und Feature Release.

Tabelle 32: Vergleich von Long Term Support (LTS) Release und Feature Release

Kategorie	Long Term Support (LTS) Release	Feature Release
Release-Frequenz	Alle 36 Monate (umfasst Fehlerbehebungen und sicherheitsrelevante Aktualisierungen).	Ungefähr alle 12 Monate (umfasst Fehlerbehebungen und sicherheitsrelevante Aktualisierungen).
Dauer uneingeschränkter Support	36 Monate	18 Monate
Dauer begrenzter Support	12 Monate (nach Ablauf des uneingeschränkten Supports)	6 Monate (nach Ablauf des uneingeschränkten Supports)
Versionierung	Alle Versionen, bei denen die zweite Ziffer **0** ist. Zum Beispiel: 9.0.0 (9.0.1, 9.0.2,), 10.0.0, 11.0.0, und so weiter.	Alle Versionen, bei denen die zweite Ziffer **nicht 0** ist. Zum Beispiel: 9.1.0 (9.1.1, 9.1.2), 9.2, 9.3, und so weiter.
Verfügbarkeit von Service Packs zwischen Releases	Ungefähr alle 6 Monate werden kumulative Updates (CUs) für jede LTS-Version erwartet.	Alle 6 Monate werden Patch Releases (Service Pack) für jeden derzeit unterstützten Feature Release erwartet.
Kriterien für die Bereitstellung von Hotfixes für LTS außerhalb eines kumulativen Aktualisierungszyklus	• Das Produkt funktioniert nach der Installation des letzten CUs nicht mehr und der Kunde kann nicht warten, bis das nächste CU verfügbar ist. • Das Produkt funktioniert nicht/ist nicht funktionsfähig, was zu einem Produktionsausfall/einem schwerwiegenden Problem führt.	

Kategorie	Long Term Support (LTS) Release	Feature Release
	• Eine sicherheitsrelevante Korrektur wird dringend benötigt, um eine Schwachstelle zu beheben. • Es werden keine Korrekturen zur Umsetzung einer Verbesserung außerhalb des kumulativen Aktualisierungszyklus herausgeben.	

Details zu den Releases finden Sie unter Product Life Cycle.

One Identity empfiehlt dringend, immer die neueste Version des gewählten Release-Pfads (Long Term Support-Pfad oder Feature Release-Pfad) zu installieren.

Wechsel zwischen LTS-Versionen und Feature Release-Versionen

Sie können von einer LTS-Version (zum Beispiel 9.0 LTS) wechseln, indem Sie ein späteres Feature Release oder eine spätere Version (zum Beispiel 9.2) installieren. Sobald dies geschieht, sind Sie nicht mehr auf dem LTS-Support, bis die nächste LTS-Basisversion (zum Beispiel 10.0) installiert ist.

Sie können von einem Feature Release zu einem LTS Release wechseln, aber nur zu einem LTS Release mit einer späteren Version. Sie können zum Beispiel nicht von Version 9.2 auf 9.0 LTS wechseln. Sie müssen mit jedem neuen Feature Release ein Upgrade durchführen, bis die nächste LTS Release-Version veröffentlicht wird. In diesem Beispiel würden Sie warten, bis 10.0 LTS verfügbar ist.

Patches

Für LTS werden keine Patches veröffentlicht, sondern nur Hotfixes. Diese werden nur in seltenen Fällen verteilt. Die Kriterien für LTS-Hotfixes entnehmen Sie bitte der vorherigen Tabelle. Diese Hotfixes müssen in der Reihenfolge ihrer Veröffentlichung angewendet werden.

Für LTS-Kunden werden in regelmäßigen Abständen kumulative Updates (CUs) bereitgestellt, welche die während dieses Zeitraums vorgenommenen Korrekturen zusammenfassen. Es ist nicht erforderlich, jedes CU einzeln zu installieren. Wenn beispielsweise CU 1 veröffentlicht wird und anschließend CU 2, müssen Sie nicht CU 1 installieren, bevor Sie CU 2 installieren. Die CUs sind kumulativ.

Für Kunden, die sich für die Feature Release-Option entschieden haben, sind die Wartungsversionen kumulativ, das heißt es müssen keine Zwischenversionen installiert werden, um eine neuere Wartungsversion zu erhalten. Dies ist gegenüber früheren Versionen unverändert. Wenn Sie beispielsweise 9.1.1 verwenden und auf 9.2 umsteigen möchten und beispielsweise die Versionen 9.1.3, 9.1.4 und 9.1.5 veröffentlicht wurden,

können Sie einfach Version 9.2 installieren, die automatisch die Korrekturen von 9.1.3, 9.1.4 und 9.1.5 übernimmt.

Häufig gestellte Fragen (FAQs)

Was ist langfristiger Support (LTS)?

- Bei LTS handelt es sich um eine Support-Option, bei der Sie über einen längeren Zeitraum auf derselben Version verbleiben können, während Sie weiterhin das hohe Maß an Support erhalten, für das One Identity bekannt ist. Während der LTS-Phase erhalten Sie Updates zur Behebung von Fehlern und Sicherheitslücken. Während der LTS-Version werden jedoch keine Produktverbesserungen oder Funktionen bereitgestellt.

Was sind die Vorteile einer LTS-Version?

- Für einige Unternehmen ist es schwierig, mit der Migration auf neue Versionen rechtzeitig Schritt zu halten, um die Support-Richtlinien des Herstellers einzuhalten. Auf diese Weise kann das Unternehmen über einen längeren Zeitraum auf einer Version bleiben.

Was sind die Nachteile einer LTS-Version?

- Der Nachteil ist natürlich, dass man nicht die neuesten Verbesserungen und Funktionen des Herstellers erhält.

Dauer einer LTS-Version

- Eine Long Term Support (LTS)-Version bietet Ihnen bis zu 3 Jahre Support nach dem ursprünglichen Veröffentlichungsdatum oder bis zur nächsten LTS-Version (je nachdem, welches Datum später liegt); mit der Option, den Support über den Extended Security Support (ESS) fortzusetzen.

Wie erfolgt der Wechsel zur LTS-Supportoption?

- Wenn Sie eine LTS-Version installieren, wie zum Beispiel One Identity Manager 9.0, sind Sie automatisch auf der LTS-Version. Die Wahl, die Sie für die nächste installierte Version treffen, bestimmt, ob Sie auf der LTS-Version bleiben oder zum traditionellen Support-Modell wechseln.

Kann ich, wenn ich mich für die LTS-Version entschieden habe, jemals wieder zum Feature Release wechseln?

- Ja. Dies kann durch die Installation einer späteren Wartungs- oder Funktionsversion geschehen. Wenn Sie beispielsweise 9.0 (LTS) verwenden und sich für 9.2 entscheiden, verlassen Sie den LTS-Support-Pfad, bis die nächste LTS-Basisversion (10.0 und so weiter) installiert ist.

Entstehen zusätzliche Kosten, wenn ich mich für die LTS-Option entscheide?

- Nein, der Langzeit-Support ist in Ihrer jährlichen Wartungsverlängerung enthalten. Eine Option zur Fortsetzung des eingeschränkten Supports wird gegen eine zusätzliche Gebühr über unseren Extended Security Support (ESS) angeboten.

Produktlizenzierung

Die Verwendung dieser Software wird geregelt durch den Software Transaktionsvertrag unter https://www.oneidentity.com/legal/sta.aspx. Diese Software erfordert für den Betrieb weder einen Aktivierungs- noch einen Lizenzschlüssel.

Upgrade und Installationsanweisungen

Um One Identity Manager 9.2 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 84.

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 9.2 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 9.2 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\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 mit der Version 9.2 sowie der Aktualisierung einer One Identity Manager-Datenbank von Version 8.0.x auf die Version 9.2 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 9.2 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.

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

Aktualisieren des One Identity Manager auf Version 9.2

> WICHTIG: Beachten Sie die Hinweise zur Aktualisierung des One Identity Manager auf Seite 84.

Um eine bestehende One Identity Manager Installation auf die Version 9.2 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.
    c. Klicken Sie **Installieren**.

       Der Installationsassistent wird gestartet.
    d. Folgen Sie den Installationsanweisungen.

       WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
3. Beenden Sie den One Identity Manager Service auf dem Aktualisierungsserver.
4. Erstellen Sie eine Sicherung der One Identity Manager-Datenbank.
5. Prüfen Sie, ob der Kompatibilitätsgrad der Datenbank auf den Wert **150** eingestellt ist und passen Sie die Wert bei Bedarf an.
6. Führen Sie die Schemaaktualisierung der One Identity Manager-Datenbank aus.
    - Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation und folgen Sie den Anweisungen.

      Verwenden Sie für die Aktualisierung des One Identity Manager Schemas mit dem Configuration Wizard einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.
        - Verwenden Sie denselben Benutzer, den Sie auch für die initiale Schemainstallation verwendet haben.
        - Haben Sie bei der Schemainstallation einen administrativen Benutzer erstellt, dann verwenden Sie diesen Benutzer.
        - Haben Sie zur Schemainstallation einen Benutzer mit Windows-Authentifizierung gewählt, dann müssen Sie diesen Benutzer zur Aktualisierung verwenden.

      HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 9.2 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.
   c. Klicken Sie **Installieren**.

      Der Installationsassistent wird gestartet.
   d. Folgen Sie den Installationsanweisungen.

      WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
8. Prüfen Sie die Anmeldeinformationen des One Identity Manager Service. Geben Sie das zu verwendende Dienstkonto an.
9. Starten Sie den One Identity Manager Service auf dem Aktualisierungsserver.
10. Aktualisieren Sie weitere Installationen auf Arbeitsstationen und Servern.

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

Um Synchronisationsprojekte auf die Version 9.2 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 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 90.

Um einen Anwendungsserver auf die Version 9.2 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 9.2 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 9.2 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 9.2 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 Änderungen aus der Version 9.2 in Ihre HTML-Anwendungen zu übernehmen

1. Laden Sie den aktuellen Stand des Quelltextes vom Github-Repository von One Identity.
2. Übernehmen Sie die Änderungen am Quelltext aus dem Branch **v92** in Ihr Repository.
3. Kompilieren Sie Ihre HTML-Anwendungen und beheben sie eventuell auftretende Kompilierfehler.

   Ausführliche Informationen finden Sie im *One Identity Manager HTML5-Entwicklungshandbuch*.
4. Prüfen Sie, ob Ihre HTML-Anwendungen noch ordnungsgemäß funktionieren.

5. Stellen Sie die neue Version Ihrer HTML-Anwendungen bereit.

   Ausführliche Informationen finden Sie im *One Identity Manager HTML5-Entwicklungshandbuch*.

Um die Manager-Webanwendung auf die Version 9.2 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 Bearbeitungsberechtigungen auf das Installationsverzeichnis der Manager-Webanwendung. Prüfen Sie, ob die entsprechenden Berechtigungen vorhanden sind.

Anwenden von Patches für Synchronisationsprojekte

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

Bevor Sie einen Patch anwenden

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

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

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

Um Patches anzuwenden

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie das Menü **Bearbeiten > Synchronisationsprojekt aktualisieren**.

3. Wählen Sie im Bereich **Verfügbare Patches** die Patches aus, die angewendet werden sollen. Mehrfachauswahl ist möglich.

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

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

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

Siehe auch:

- Änderungen an Synchronisationsvorlagen auf Seite 60
- Patches für Synchronisationsprojekte auf Seite 63

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 2023.0009.0002.0000 für alle Module und die Anwendungsversion 9.2 v92-226554 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 Kunden von One Identity 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.