One Identity Manager 8.2.1

Versionshinweise

29. April 2022, 10:28 Uhr

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 8.2.1 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 8.2 aufgeführt.

One Identity Manager 8.2.1 ist ein Patch Release mit neuen Funktionen und verbessertem Verhalten. Siehe Neue Funktionen auf Seite 2 und Verbesserungen auf Seite 6.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 8.2 ist, lesen Sie auch die Versionshinweise der vorangegangenen Versionen. Die Versionshinweise sowie Versionshinweise zu zusätzlichen Modulen, die auf der One Identity Manager-Technologie basieren, finden Sie unter One Identity Manager Support.

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

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

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Über One Identity Manager 8.2.1

One Identity Manager vereinfacht konzernweit den Prozess der Verwaltung von Benutzeridentitäten, Zugriffsberechtigungen und Sicherheitsrichtlinien. Sie ermöglichen den Unternehmen die Kontrolle über Identitätsverwaltung und Zugriffsentscheidungen, während sich die IT-Teams auf ihre Kernkompetenzen fokussieren können.

Mit diesen Produkten können Sie:

- Gruppenverwaltung mittels Selbstbedienung und Attestierung für Active Directory mit der One Identity ManagerActive Directory Edition umsetzen,
- Access Governance Anforderungen in Ihrem gesamten Konzern plattformübergreifend mit dem One Identity Manager verwirklichen.

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

One Identity Starling

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

Neue Funktionen

Neue Funktionen in One Identity Manager 8.2.1.

Allgemein

- Die Verarbeitung der internen DBQueue Prozessor Aufträge kann durch einen Dienst, den Database Agent Service, erfolgen. Der Database Agent Service wird über ein Plugin des One Identity Manager Service bereitgestellt. Das DatabaseAgentPlugin sollte auf dem Jobserver konfiguriert sein, der die Funktion des Aktualisierungsservers übernimmt. Für die Datenbankverbindung im Jobprovider muss ein administrativer Benutzer verwendet werden. Alternativ kann der Database Agent Service über das Kommandozeilenprogramm `DatabaseAgent.exe` ausgeführt werden.

Sie können während der Installation oder Aktualisierung einer Datenbank mit dem Configuration Wizard wählen, ob der Database Agent Service oder weiterhin der SQL Server Agent die internen Aufträge der Datenbank verarbeiten soll. Welcher Agent genutzt wird, wird im Überblick über die Systemkonfiguration angezeigt.

> WICHTIG: Dies ist eine EXPERIMENTELLE Funktion. Ihre Auswirkungen auf die Performance von Produktionssystemen sind noch nicht bekannt. Daher wird diese Funktion noch nicht vom Support abgedeckt. Sie können die Funktion jedoch gern ausprobieren (vorzugsweise auf nicht produktiven Systemen) und Ihre Anmerkungen an OneIM.Beta@oneidentity.com senden.

- Die Abfrage von Secrets in Parametern für Prozessschritte wird unterstützt. Syntax: `&SECRET(Name)&`

  In der Konfiguration des One Identity Manager Service werden die Secrets, die für die Ersetzung zulässig sind, im Parameter `SecretsAllowList` angegeben. Im Parameter `SecretsFolder` wird das Verzeichnis angegeben, in dem die Secrets-Dateien liegen.
- Die Abfrage von Umgebungsvariablen in Parametern für Prozessschritte wird unterstützt. Syntax: `&ENV(Variablenname)&`
- In der Konfiguration des One Identity Manager Service können im Parameter `HTTPHeaders` die HTTP Header für die Statusseite konfiguriert werden.
- Es wird ein Kommandozeilenprogramm `DBConsCheckCmd.exe` für die Ausführung von Konsistenzprüfungen bereitgestellt.
- Um Eigenschaften für die Bearbeitung zu sperren, benötigen die Benutzer nun die Programmfunktion **Ermöglicht das Setzen einer Änderungssperre für bestimmte Eigenschaften einzelner Objekte** (`Common_AllowPropertyLocks`).

  Soll es bestimmten Benutzern möglich sein, Eigenschaften für die Bearbeitung zu sperren, können Sie die Berechtigungen über Berechtigungsgruppen an die Benutzer vergeben. Für die nicht-rollenbasierte Anmeldung wird die Berechtigungsgruppe **QBM_PropertyLock** bereitgestellt. Für die rollenbasierte Anmeldung wird die Anwendungsrolle **Basisrollen |Sperren einzelner Eigenschaften** bereitgestellt.

Webanwendungen

- Die Heuristik zur Erkennung von Zeitzonen wurde geändert, um Browser-Standards zu verwenden.
- Es wurde ein Code-Beispiel hinzugefügt, das zeigt, wie man einen Multi-Faktor-Authentifizierungs-Provider für die Sitzungsauthentifizierung integriert.
- Es ist nun möglich, benutzerdefinierte Varianten von Standard-HTML-Anwendungen (zum Beispiel das Web Portal) hochzuladen und zu hosten.
- Für HTML-Anwendungen ist es über eine Konfiguration im Administration Portal möglich, lokale Änderungen in globale Änderungen umzuwandeln.
- Im Administration Portal kann ein eigenes Logo für das Web Portal festgelegt werden.
- Im Kennwortrücksetzungsportal ist es nun möglich, sich als neuer Benutzer zu registrieren beziehungsweise ein neues Benutzerkonto zu erstellen.

- Im Web Portal für Betriebsunterstützung ist es nun möglich, die Anzahl der Prozesse pro Queue in einer Tabelle sowie in einem Diagramm darzustellen.
- Provisionierungsprozesse können im Web Portal für Betriebsunterstützung manuell behandelt werden.
- Es ist nun möglich, im Web Portal weitere zusätzliche Spalten und Informationen in Tabellen anzuzeigen (konfigurierbar im Administration Portal).
- Im Web Portal können dynamische Rollen für Mitgliedschaften konfiguriert werden.
- Im Web Portal ist es nun möglich, Bestellvorlagen zu verwalten und für Bestellungen zu verwenden. Es können eigene Bestellvorlagen erstellt werden.
- Im Web Portal können Eigentümer für Geräte zugewiesen werden. Es ist möglich die Eigentümerschaft für Geräte zu übernehmen.
- Im Web Portal ist es nun möglich, neue Identitäten zu erstellen.
- Die Historie einer Identität kann im Web Portal angezeigt werden.
- Es ist nun möglich, im Web Portal Regelverletzungen anzuzeigen und Ausnahmen zu erteilen oder zu verweigern.
- Im Web Portal können nun Complianceregeln angezeigt werden.
- Im Web Portal ist es nun möglich, neue SharePoint Gruppen zu bestellen.
- Im Web Portal können jetzt Berichte verwaltet werden (erstellen, bearbeiten, löschen).
- Neue Funktionen im Web Portal für Standorte, Abteilungen, Kostenstellen, Anwendungsrollen, Geschäftsrollen und Systemrollen.
    - Es können Regelverletzungen für Standorte, Abteilungen, Kostenstellen, Anwendungsrollen, Geschäftsrollen und Systemrollen angezeigt werden.
    - Abteilungen, Standorte, Kostenstellen, Geschäftsrollen, Systemrollen können im Web Portal geteilt werden.
    - Es ist möglich, Abteilungen, Standorte, Kostenstellen, Geschäftsrollen, Systemrollen miteinander zu vergleichen.
- Im Web Portal wird angezeigt, welche Berechtigungen verloren gehen, wenn ein Attestierungsvorgang abgelehnt wird.
- Es ist im Web Portal nun möglich, Entscheidung von Attestierungsvorgängen und Bestellungen zu eskalieren.
- Im Web Portal können offene Bestellungen, die andere entscheiden müssen, über eine Kachel auf der Startseite angezeigt werden.
- Im Web Portal ist es nun möglich, die komplette Merkliste zu löschen.

Zielsystemanbindung

- Unterstützung von One Identity Active Roles Version 7.5.
- Der Microsoft Exchange Konnektor kann die Attributerweiterungen (`CustomAttibute 1` bis `CustomAttibute 15`) für Postfächer, E-Mail Benutzer, E-Mail Kontakte,

Verteilergruppen und dynamische Verteilergruppen lesen und schreiben. Um die Funktionalität zu nutzen, passen Sie das Mapping an.

- Es gibt die Möglichkeit Daten zu priorisieren, wenn der Konnektor bei der Synchronisation in die One Identity Manager-Datenbank Konflikte zwischen Datenbank und Zielsystem erkennt.
- Wenn One Identity Safeguard zur Kennwortverwaltung genutzt wird, können nun Beispielskripte genutzt werden.
- Im Synchronization Editor werden Code-Ausschnitte bereitgestellt, die als Vorlage genutzt werden können, um das Kennwort für einen Systembenutzer aus einem externen Kennwortmanagementsystem auszulesen. Diese Code-Ausschnitte können genutzt werden, wenn One Identity Safeguard zur Kennwortverwaltung eingesetzt wird. Die Code-Ausschnitte können beim Erstellen von Skriptvariablen ausgewählt und kundenspezifisch angepasst werden.
- Der Azure Active Directory Konnektor kann die Schemaeigenschaft `creationType` für den Schematyp `User` lesen. Um die Funktionalität zu nutzen, passen Sie das Mapping an.

Identity Management und Access Governance

- Entscheidung von Bestellungen und Attestierungsvorgängen über Starling Cloud Assistant.

  Um Entscheidern und Attestierern, die zeitweilig keinen Zugang zu den One Identity Manager Werkzeugen haben, die Möglichkeit zu geben Bestellungen und Attestierungsvorgänge zu entscheiden, können adaptive Karten genutzt werden. Starling Cloud Assistant übermittelt die adaptiven Karten an die Entscheider und Attestierer, wartet auf deren Antwort und sendet die Antwort an den One Identity Manager. In Starling Cloud Assistant werden die Übermittlungskanäle konfiguriert und können für jeden Empfänger separat festgelegt werden. Aktuell können Slack und Microsoft Teams genutzt werden.

  Für Entscheidungen und Attestierungen über adaptive Karten wird an den Entscheidungsschritten, Leistungspositionen oder Servicekategorien festgelegt, ob bei der Entscheidung eine Begründung angegeben werden muss.

  Adaptive Karten ersetzen die Entscheidung über die Starling 2FA App. Die Unterstützung der Starling 2FA App für die Entscheidung von Bestellungen ist in der Version 8.2.1 noch enthalten, jedoch inaktiv. Starling 2FA App wird mit der nächsten One Identity Manager Version komplett entfernt. Weitere Informationen finden Sie unter Abgekündigte Funktionen auf Seite 47.
- Zertifizierung neuer Geschäftsrollen, Organisationen und Anwendungsrollen.

  Über die Attestierungsfunktion können die Stammdaten von Geschäftsrollen, Organisationen und Anwendungsrollen, die neu in One Identity Manager angelegt werden, durch deren Manager attestiert und zertifiziert werden. Der initiale Zertifizierungsstatus wird über die Konfigurationsparameter **QER | Attestation | <...> | InitialApprovalState** gesetzt. Für Rollen mit dem Zertifizierungsstatus **Neu** wird die Attestierung gestartet und entsprechend dem Ergebnis der Zertifizierungsstatus aktualisiert.

Siehe auch:

- Verbesserungen auf Seite 6
- Gelöste Probleme auf Seite 12
- Schemaänderungen auf Seite 29
- Patches für Synchronisationsprojekte auf Seite 32

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die im One Identity Manager 8.2.1 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Die Option **Abbestellen erlaubt** (`DialogRichMail.AllowUnsubscribe`) kann für Standard-Mailvorlagen kundenspezifisch angepasst werden.	34925
Verbesserte Darstellung der Änderungsinformationen des Parameters `CausingEntityPatch` im Job Queue Info. Dieser Parameter enthält den Patch, der die zu provisionierenden Änderungen enthält.	34969
Tritt im Job Queue Info bei der Statusabfrage für Jobserver ein Fehler auf, wird dies jetzt angezeigt. Über das Kontextmenü wird eine detaillierte Fehlermeldung angezeigt.	35324
Die Dokumentation kann jetzt im Launchpad angezeigt werden.	34994
Verbesserter Berechtigungen für die Berechtigungsgruppe **QBM_ BaseRight**.	35048
Die Informationen zu Feiertagen wurde aktualisiert.	35063
Anpassung der Bit-Positionen für die Herkunft einer Zuweisung (Spalte `XOrigin`) für Zuweisungstabellen. Die Bit-Position **2** für Zuweisungen über eine dynamische Rolle wurde entfernt.	35193, 35203, 35206
Unterstützung von Kerberos für die HTTP-Authentifizierung am Jobserver.	35377
Performanceverbesserung bei der Mengenverarbeitung von DBQueue Prozessor-Aufträge bei sehr großen Datenmengen.	34690
Performanceverbesserung bei der erneuten Kompilierung der Ausführungspläne für den DBQueue Prozessor.	34803, 34813
Verbesserter Sicherheitseinstellungen für die Dokumentation.	35225
Verbesserter Test zur Verhinderung von Blind-SQL Injections.	35166

Verbesserung	Fehler ID
Verbesserte Sicherheit bei der Protokollierung von Anmeldeversuchen.	35230
Die Drittanbieterkomponente `DevExpress` wurde aktualisiert.	35296

Aus Sicherheitsgründen kann das HTML-Frontend des Anwendungsservers abgeschaltet werden. Fügen Sie dazu folgenden Eintrag in die Konfigurationsdatei in der `<server>`-Sektion ein.
`<!-- Do not provide the HTML/JS frontend -->`
`<add key="nofrontend" value="true" />`
Damit ist auch die API Dokumentation im Anwendungsserver inklusive der Testmöglichkeiten nicht mehr verfügbar.
	35345

Aus Sicherheitsgründen kann das HTML-Frontend des One Identity Manager Service abgeschaltet werden. Tragen Sie dazu in den Parameter `HTTP server IP address` die IP Adresse des Localhost (127.0.0.1) ein.	35345
Der Anwendungsserver zeigt eine Fehlermeldung **406 Not Acceptable**, wenn der angeforderte Content-Type nicht unterstützt wird.	35314
Der Konfigurationsparameter **QER | Person | PasswordResetAuthenticator | SearchColumn** wurde so erweitert, dass man nun mehrere Spalten angeben kann. Die Spalten können mit Pipe (**|**) getrennt angegeben werden.	34116

Tabelle 2: Webanwendungen

Verbesserung	Fehler ID
Das Web Portal prüft, ob durch die Bestellung einer Zuweisung an Geschäftsrollen und Organisationen Complianceregeln verletzt werden können, auch wenn keine Person direkt davon betroffen ist. Diese Prüfung kann nun deaktiviert werden.	35163
Im Web Portal für Betriebsunterstützung wurde die Anzeige der Prozesse und die Filtermöglichkeiten verbessert.	293072
Im Web Portal können jetzt Anwendungen gelöscht werden.	261577
Im Web Portal werden Details von Produkten angezeigt, wie beispielsweise Stichworte, Beschreibung, Berechtigungstyp und vererbte Berechtigungen.	279436
Im Web Portal ist es nun möglich, Berichte direkt im Browser anzuzeigen.	293386
In der Bestellhistorie im Web Portal werden nun Compliance-Verletzungen angezeigt.	294063
Im Web Portal ist es nun möglich, einem Regal eines Shops zusätzlich Berichte, Kontendefinitionen und unwirksame Azure Active Directory Dienstpläne hinzuzufügen.	294072
Das Bestellen für andere Identitäten im Web Portal wurde überarbeitet.	294912,

Verbesserung	Fehler ID
	30104
Im Web Portal können Benutzerkonten und Systemberechtigungen nach Zielsystem und Container gefiltert werden.	296472
Im Web Portal werden Regelverletzungen für Attestierungsvorgänge angezeigt.	297245
Im Web Portal ist es nun möglich, weitere Informationen wie Mitgliedschaften, Regelverletzungen, Berichte und Zuweisungsanalysen anzuzeigen.	298169
Die Performance des Web Portals wurde verbessert.	31057
Die Inhalte der Kachel **Attestierung meiner Berechtigungen** auf der Startseite des Web Designer Web Portals wurden verbessert.	30350
Im Web Designer Web Portal werden nun in den Stammdaten von Rollen keine leeren Verzeichnisse mehr angezeigt.	35066

Anwendungen müssen sich nun mit einem speziellen Schlüssel (`Trusted Source Key`) authentifizieren. Bei der initialen Installation wird der Trusted Source Key automatisch konfiguriert.
Nach der Aktualisierung von One Identity Manager auf die Version 8.2.1 müssen Sie aktiv den Trusted Source Key konfigurieren.
Um den Trusted Source Key zu konfigurieren
1. Öffnen Sie auf dem Server mit der installierten Webanwendung ein Kommandozeilenprogramm mit Administratorrechten.
2. Wechseln Sie in ein Verzeichnis mit installierten One Identity Manager-Entwicklungswerkzeugen.
3. Rufen Sie folgenden Befehl auf:
`imxclient edit-config /path <Pfad zur web.config-Datei> -T`
(zum Beispiel `imxclient edit-config /path c:\inetpub\wwwroot\apiserver\web.config -T`)
oder
`imxclient edit-config /path <Pfad zur web.config-Datei> /trustedsourcekey <Key>`
	301102

Im Administration Portal lässt sich nun konfigurieren, ob bei einer Bestellung über eine Peer-Gruppe nur Produkte angezeigt werden, die bereits innerhalb der Peer-Gruppe bestellt wurden.	295703
Im Administration Portal lässt sich nun die Benutzung des Auth Tokens über die Konfiguration abschalten.	301952, 35271

Verbesserung	Fehler ID
Die Sicherheit für StsSetup wurde erhöht.	300583
Der RSTS wurde auf die Version 2022-03-30.1 aktualisiert.	305080
Die Übermittlung von Log-Einträgen vom Webclient zum Server kann nun abgeschaltet werden. Fügen Sie dazu in die Datei `web.config` unter `<appSettings>` den folgenden Eintrag ein: `<add key="DisableClientLog" value="true" />`	34937

Tabelle 3: Zielsystemanbindung

Verbesserung	Fehler ID
Der Zeitpunkt, an dem die Synchronisation beendet wurde, wird im Synchronisationsprotokoll aufgezeichnet.	34841
Das Kennwort des Synchronisationsbenutzers für die Synchronisation von Oracle E-Business Suite-Umgebungen wird als Variable gespeichert und kann auf einer verschlüsselten Datenbank separat verschlüsselt werden. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34775 bereitgestellt.	34775
In das *One Identity Manager Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung* wurde eine Liste der SAP Benutzerkonten aufgenommen, die im One Identity Manager nicht bearbeitet werden können.	35331
Verbesserte Unterstützung der Synchronisation von Tochtersystemen einer ZBV, die sich nicht im selben SAP System befinden, wie das Zentralsystem. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35118 bereitgestellt.	35118
Verbesserte Unterstützung von dynamischen Gruppen in Azure Active Directory.	34777
Verbesserte Abbildung des Empfängertyps eines Exchange Online E-Mail Benutzers. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34938 bereitgestellt.	34938
Der Active Roles Konnektor kann das Benutzerkonto des One Identity Manager Service zur Anmeldung am Zielsystem nutzen. Dazu wird im Projektassistenten auf der Seite **Anmeldeinformationen** die Option **Aktuelle Anmeldedaten verwenden (aktueller Benutzer/Dienstkonto)** aktiviert.	34391
Verbesserte Unterstützung der Microsoft Exchange Postfachberechtigungen **Senden als** und **Vollzugriff**. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID	21073

Verbesserung	Fehler ID
VPR#21073_2 bereitgestellt.	
Verbesserte Prüfung der Eindeutigkeit der E-Mail-Adresse für Remotepostfächer.	35080
Auf den Übersichtsformularen für LDAP Benutzerkonten, LDAP Gruppen und LDAP Computer wird zusätzlich die Domäne angezeigt.	34483
Bei der automatischen Bestellung von Exchange Online E-Mail aktivierten Verteilergruppen werden jetzt auch die Mitglieder einer Gruppe von Administratoren als Produkteigner übernommen.	34850
Beim Löschen von Exchange Online E-Mail aktivierten Verteilergruppen und Office 365 Gruppen sowie beim Löschen von Gruppenmitgliedschaften werden die verbundenen Azure Active Directory-Objekte ebenfalls gelöscht.	34855
Verbesserungen für die Objektsuche im Zielsystem bei der Provisionierung.	34184
Im Synchronization Editor können zusätzliche Informationen über das angebundene Zielsystem angezeigt werden.	33482
Für Konnektoren, die als obsolet gekennzeichnet sind, können keine neuen Synchronisationsprojekte mehr eingerichtet und Systemverbindungen erstellt werden.	34479
Reduzierung des Grundspeicherverbrauchs von Systemobjekten in Systemkonnektoren.	35032
Verbesserungen im Dialog zur Bearbeitung von Schemaeigenschaften im Synchronization Editor.	35252
Der Prozess `DPR_Migrate_Shell` hat eine höhere Priorität erhalten, damit er abgeschlossen ist, bevor etwaige Synchronisierungs- oder Provisionierungsprozesse starten.	34903
Fehler bei der Provisionierung in eine Google Workspace-Umgebung werden abgefangen, wenn Zuweisungen von Produkten und SKUs an Benutzerkonten geändert werden, wobei nur die Lizenz geändert wird, das Produkt jedoch identisch bleibt.	32276
Unterstützung von SAP S/4HANA auch mit SAP BASIS Version 7.53.	35279
Die Dokumentation der benötigte Berechtigungen für die Synchronisation mit einer Oracle E-Business Suite wurde verbessert.	34119
Bei Verwendung des Funktionsbausteins `/VIAENET/READTABLE` können die Zugriffsberechtigungen auf Tabellen nun auch über die Berechtigungsobjekte S_TABU_NAM oder S_TABU_DIS definiert werden. Diese werden gleichwertig geprüft.	35465

Tabelle 4: Identity Management und Access Governance

Verbesserung	Fehler ID
Performanceverbesserung bei der Ermittlung der Herkunft von Berechtigungen für Personen.	34768
Bestellparameter werden beim Löschen abgeschlossener Bestellvorgänge archiviert.	33647
Verbesserte Darstellung der Stammdaten von Attestierungsrichtlinien.	34924
Wenn das Erzeugen neuer Attestierungsvorgänge länger als 48 Stunden dauert, wird der Vorgang abgebrochen. Das Timeout für die Erzeugung von Attestierungsvorgängen kann im Konfigurationsparameters **QER | Attestation | PrepareAttestationTimeout** festgelegt werden.	34932
Verbesserte Dokumentation für das Aussetzen von Attestierungen, beispielsweise durch Deaktivieren der Attestierungsrichtlinien.	34945
Stichproben können im Manager nur noch in der Kategorie Attestierung bearbeitet werden.	35108
Verbesserte Darstellung der Zuordnung von Bestelleigenschaften und Bestellparametern an Leistungspositionen und Servicekategorien im Manager.	35148
Auf Oberflächenformularen im Manager werden potentielle Regelverletzungen besser dargestellt. Das Formularelement für Zuweisungen, die potentiell zu Regelverletzungen führen können, wurde umbenannt.	35147
Nach einem Import von HR-Daten werden Bildungsregeln an verschiedenen Spalten an Person nur ausgeführt, wenn der Import diese Daten nicht geändert hat.	34842
Die Konsistenzprüfung **Missing default entries in QERRiskIndex** wurde verbessert.	35411
Für die Tabelle `PersonHasQERResource` ist die Zuweisung per Ereignis (`IsAssignmentWithEvent`) jetzt standardmäßig aktiviert.	35452

Siehe auch:

- Schemaänderungen auf Seite 29
- Patches für Synchronisationsprojekte auf Seite 32

Gelöste Probleme

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

Tabelle 5: Allgemein

Gelöstes Problem	Fehler ID
Performanceprobleme bei der Überprüfung der eindeutigen Gruppen beim Einfügen von Objekten.	34830
Der One Identity Manager Service bemerkt Änderungen an der Option Dienstkonto für seinen Systembenutzer (Spalte `DialogUser.IsServiceAccount`) nicht.	34858
Die Übernahme aus dem DBQueue Puffer (Tabelle `QBMDBQueuePond`) in die DBQueue scheitert aufgrund zu großer in-memory-Tabellen.	34867
Unter Umständen tritt bei der Berechnung von Tabellenstatistiken ein Fehler auf.	34888
Die Reparatur des Suchindex auf dem Anwendungsserver funktioniert unter Umständen nicht.	34894
Der One Identity Manager Service kann nicht initialisiert werden, wenn es inkonsistente Prozesse in der Jobqueue gibt. Mit dieser Fehlerbehebung werden inkonsistente Prozesse jetzt in der Prozesshistorie aufgezeichnet.	34897
Fehler beim Bestimmen der Anzeigewerte in einfachen Listenberichten.	34923
Fehler beim Öffnen der Prozessinformationen im Manager, wenn das Programm über den Anwendungsserver verbunden ist.	34942
Der Anwendungsserver zeigt auf der Statusseite immer den Wert **-1** für die Softwarerevision.	34988
Im Configuration Wizard ist auf der Seite **Lieferantenbenachrichtigung konfigurieren** die **Zurück**-Schaltfläche aktiv.	34989
Fehler während der gleichzeitigen Ausführung mehrerer Datenarchivierungen. Fehlermeldung: `The instance of the SQL Server Database Engine cannot obtain a LOCK resource at this time. Rerun your statement when there are fewer active users.`	35016
Fehlerhafter Wert von **maximum degree of parallelism (DB)** im Überblick über die Systemkonfiguration.	35022
Wenn die Spalte `DialogDatabase.ConnectionString` mit der Option **Blob (external)** (`isBlobExternal = 1`) gekennzeichnet ist, schlägt die Generierung jeglicher Prozesse fehl. Fehlermeldung: `Value ConnectionString was not found.`	35043

Gelöstes Problem	Fehler ID
Bei Einsatz eines SQL Server mit der Version 2019 werden wesentliche Einstellungen für die Datenbank nicht aktiviert.	35084
Performanceprobleme bei de Berechnung der Sortierreihenfolge von DBQueue Prozessor Aufträgen.	35087
Bei der Aktualisierung des Ausführungsstatus eines Prozessschritte wird das Änderungsdatum nicht angepasst.	35095
Performanceprobleme, wenn bei der Mengenverarbeitung von DBQueue Prozessor Aufträgen der Mechanismus zum Schutz vor Überladung eingesetzt wird.	35103
Performanceprobleme bei der Berechnung einer sehr großen Anzahl von Gruppenmitgliedschaften.	35104
Die Einträge der Prozesshistorie werden zu früh gelöscht oder zu früh in die History Database verschoben.	35136
Der Objektschlüssel (Spalte `XObjectKey`) für die Zeitzone **Kanton** ist fehlerhaft.	35150
Während der Migration werden Bitmasken von kundendefinierten Spalten nicht in die Tabelle `QBMColumnBitMaskConfig` übernommen.	35159
Parameter ohne Werte werden beim Generieren von Prozessen ignoriert.	35173
Fehler beim Speichern verzögerter Operationen, wenn die Daten Zeilenumbrüche enthalten.	35204
Das Importieren von Dateien mit Platzhaltern in Unterverzeichnissen funktioniert im Kommandozeilenprogramm `SoftwareLoaderCMD.exe` nicht.	35299
Beim Importieren von Daten über ein Importskript im Data Import werden Datumsangaben und Zeitangaben unter Umständen geändert.	35312
Die Migration auf Version 8.2 scheitert bei sehr vielen Änderungen von UIDs.	35336, 35030
Aktivieren der Option **Aufzeichnen von Änderungen** (Spalte `IsToWatch`) auf eine `timestamp`-Spalte führt zum Fehler bei der Generierung der *Watch-Trigger.	35384
Die Datei `VI.Projector.ScriptSupport.dll` wird nicht auf dem Jobserver installiert.	34951
Speichern eines abhängigen Objektes im `OnSaved`-Skript führt zu Fehler.	35446
Unter Umständen wird für einen Wert die falsche Übersetzung angezeigt.	35436
Fehler beim Verschlüsseln einer Datenbank, wenn das Kennwort in einer Zielsystemverbindung doppelte Anführungszeichen enthält.	35408

Tabelle 6: Webanwendungen

Gelöstes Problem	Fehler ID
Bestimmte Sonderzeichen im Datenbankkennwort verursachen Fehler beim Installieren des Web Designer Web Portals.	34294
Im Web Designer Web Portal kann im Filterassistenten kein Datum verwendet werden.	34435
Der Zähler für gefilterte Ergebnisse ist unzutreffend, wenn die Ergebnisse über mehrere Seiten dargestellt werden würden. Das Paging steht nach dem Filtern nicht mehr zur Verfügung.	34506
Die Beschriftungen für die Gruppierungsspalten und Eigenschaften von Attestierungsvorgängen werden im Web Designer Web Portal auf der Seite **Mein Attestierungsstatus** nicht korrekt angezeigt.	34593
Im Web Designer kann die Eigenschaft **Maximale Dateilänge** nicht für Komponenten verwendet werden, mit denen Dateien hochgeladen werden sollen.	34840
Im Web Designer Web Portal werden in Auswahllisten statt den Namen von Abteilungen deren IDs angezeigt.	34943
Im Web Designer Web Portal kommt es beim Bearbeiten der Ansichtseinstellungen einer Seite zum Fehler.	34983
Kundenspezifische Dateien werden wird bei Installation eines API Servers im falschen Verzeichnis abgelegt.	35050
Im Web Designer Web Portal kann man im Filterassistent des Adressbuchs keine Objekte auswählen.	35052
Im Web Designer Web Portal und im Web Portal kann nicht nach Produkten/Leistungspositionen mit Doppelpunkt im Namen gesucht werden.	35100, 35309
Im Web Portal werden Daten nach vorheriger Einschränkung nicht korrekt eingeschränkt. Beispielsweise werden nach Auswahl einer Abteilung Identitäten angezeigt, die nicht der gewählten Abteilung angehören.	35124
Im Web Designer Web Portal wird beim manuellen Angeben einer Seitenzahl in Tabellen nicht zur gewünschten Seite gewechselt, sondern stattdessen ein Fehler erzeugt.	35257
Wenn man einen Angular-Workspace in untergeordneten Ordnern anlegt, kann die HTML-Anwendung nicht mehr kompiliert werden.	35272
Im englischsprachigen Web Designer Web Portal und im Web Portal funktioniert die Suche nach Produkten/Leistungspositionen nicht korrekt.	35310
Im Web Designer Web Portal kommt es unter bestimmten Umständen bei der Anzeige der offenen Attestierungen zum Fehler.	35323

Tabelle 7: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Mitgliedschaften von Azure Active Directory Gruppen , die mit dem lokalen Active Directory synchronisiert werden (Spalte `OnPremisesSyncEnabled=True`), dürfen nicht provisioniert werden.	34448
Die Customizer für die Tabelle `AADUserInGroup` verhindern unter Umständen das Löschen einer Mitgliedschaft.	34702
Fehler bei der Ermittlung des Benutzeranmeldenamens für Azure Active Directory Benutzerkonten in Verbund-Umgebungen. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#34896 bereitgestellt.	34896
Bei der Synchronisation mit Azure Active Directory werden unter Umständen Mitgliedschaften als ausstehend markiert. Die nachfolgende Synchronisation entfernt die Markierung wieder.	35400
Falsch festgelegte Verarbeitungsmethoden in den Synchronisationsschritten **Calendar Processing** und **Mailbox Statistics** in Synchronisationsworkflows für Exchange Online. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35373 bereitgestellt.	35373
Einige Eigenschaften für Exchange Online Objekte, wie beispielsweise Grenzwerte, unterscheiden nicht zwischen den Einstellungen **0** und **unbegrenzt**. Mit dieser Fehlerbehebung wird der Wert **-1** als **unbegrenzt** interpretiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35343_O3E bereitgestellt.	35343
Fehler bei der Provisionierung von SAP Benutzerkonten, wenn dem Benutzerkonto ein Stellvertreter zugeordnet ist. Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#35370 und VPR#35370_CUA bereitgestellt.	35370
Sporadische Datenfehler bei externen Schemaerweiterungen, die auf SAP Tabellen basieren. Zwischen den selektierten Datensätzen werden Daten vermischt.	34382
An bestehenden Zuweisungen von strukturellen Profilen an SAP Benutzerkonten können das Gültig-bis-Datum und die Option **Ausschluss** nicht bearbeitet werden. Es werden Patches für Synchronisationsprojekte mit der Patch ID VPR#35174_1 und VPR#35174_2 bereitgestellt.	35174
Fehler beim Provisionieren der Eigenschaften `authOrig` für die Schemaklasse `group` in das Active Directory.	34931

Gelöstes Problem	Fehler ID
Bei der Synchronisation von Active Directory Benutzerkonten werden Einträge in der Tabelle `QBMServer` erzeugt, obwohl der Konfigurationsparameter **TargetSystem | ADS | AutoCreateServers** deaktiviert ist.	34990
Das Skript `ADS_PersonUpdate_ADSAccount` weist einer Person ein Bundesland zu, obwohl das Active Directory Benutzerkonto kein Bundesland hat.	35101
Für Active Directory Objekte wird die Eigenschaft `vrtparentDN` falsch gebildet, wenn der definierte Name des übergeordneten Objektes einen Schrägstrich (**/**) enthält.	35458
Einige Eigenschaften für Microsoft Exchange Objekte, wie beispielsweise Grenzwerte, unterscheiden nicht zwischen den Einstellungen **0** und **unbegrenzt**. Mit dieser Fehlerbehebung wird der Wert **-1** als **unbegrenzt** interpretiert. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#35343_EX0 bereitgestellt.	35343
Abholen eines Kennwortes aus One Identity Safeguard scheitert mit einer Fehlermeldung.	35429
Fehler beim Laden von Objekten aus einer Cloud-Anwendung mit dem SCIM Konnektor.	34999
Objekte, die bei der Synchronisation ignoriert wurden, weil dazu noch Prozesse in der Jobqueue vorhanden waren, werden auch bei einer darauffolgenden Synchronisation mit Revisionsfilterung nicht verarbeitet.	35049
Wenn eine Synchronisation über mehrere Tage läuft und die im Konfigurationsparameter **DPR | Journal | LifeTime** angegebene Zeit kürzer ist, wird das Synchronisationsprotokoll für die laufende Synchronisation gelöscht. Die Synchronisation wird mit einem Fehler abgebrochen.	35135
Fehler bei der Synchronisation, wenn in einem Synchronisationsschritt eine kundendefinierte Verarbeitungsmethode ausgeführt wird.	35264
Unbekannte Schematypen werden im Zielsystembrowser des Domino Konnektors nicht in der Einzelobjektansicht angezeigt.	35001
Beim Umbenennen einer Notes Gruppe wird der falsche Name in das AdminP-Anforderungsdokument geschrieben.	35021
Datentypfehler beim Lesen sehr großer Datenmengen mit dem Domino Konnektor.	35268
Wenn in einer SAP Schemaerweiterungsdatei an eine Funktion ein fester Parameter übergeben wird, wird die Ergebnisliste nicht auf den Parame-	34948

Gelöstes Problem	Fehler ID
terwert eingeschränkt.	
Fehlende Berechtigungen des Synchronisationsbenutzers für die Synchronisation mit einer SAP S/4HANA 2.0-Umgebung.	34967
Fehlende Berechtigungen auf die Tabelle `SAPUserMandant` im Kennwortrücksetzungsportal.	34986
Die Bildungsregel an der Spalte `SAPUser.Pname` wird nur für neue Objekte ausgeführt.	35083
Sperren eines SAPUsers einer CUA führt zu einer Template-Inkonsistenz für SAPUser.U_Flag Beim Sperren eines SAP Benutzerkontos in einer zentralen Benutzerverwaltung wird ein falscher Wert für den Sperrvermerk (`SAPUser.U_Flag`) gesetzt.	35156
Performanceprobleme im DBQueue Prozessor bei der Verarbeitung der Zuweisungen von Unternehmensressourcen für Personen, die mit SAP Benutzerkonten verbunden sind.	35223
`TempUserPassword` ist am Parameter `OverrideVariables` in den Prozessen `SAP_SAPUser_Insert` und `SAP_SAPUser_Update` nicht verschlüsselt.	35307
Wenn im Systemverbindungsassistenten für den Windows PowerShell Konnektor zurück geblättert wird, werden bereits erfasste Einstellungen durcheinander gebracht.	35129
Fehlermeldung beim Öffnen einer Gruppe eines kundendefinierten Zielsystems in der Manager Webanwendung.	35187
Für Spalten einer Schemaerweiterung für ein eines kundendefiniertes Zielsystem wird in der Manager Webanwendung die alternative Spaltenbezeichnung nicht angezeigt.	35284
Es ist möglich Kontendefinitionen an Benutzerkonten zuzuweisen, die als ausstehend markiert sind. Damit wird unter Umständen versucht ein weiteres Benutzerkonto zu erzeugen. Mit dieser Fehlerbehebung werden jetzt entsprechende Meldungen in das Protokoll geschrieben und der Prozess geht unter Umständen in den Status **frozen**. Bearbeiten Sie das Benutzerkonto im Zielsystemabgleich nach und starten Sie die Verarbeitung des gesamten Prozesses erneut.	35346
Im Synchronization Editor werden Tabellen zum Komprimieren angeboten, die nicht komprimiert werden können.	35397
Der CSV Konnektor konvertiert **DateTime**-Werte nicht nach UTC Zeit.	33676
Fehler beim Anzeigen von One Identity Manager Objekten im Zielsystembrowser, wenn die Verbindung zur One Identity Manager-Datenbank	35441

Gelöstes Problem	Fehler ID
mit dem **RemoteConnectPlugin** hergestellt wurde.	
Syntaxfehler beim Einspielen der One Identity Manager BAPI-Transporte. Es wird ein neuer BAPI-Transport bereitgestellt (`SAPBusinesspartnerProxies.zip`), welcher die Funktionen enthält, die im /VIAENET/HELPER-Paket definiert sind. Der Transport wird nur benötigt, wenn ein SAP S/4HANA-System angebunden wird und Geschäftspartnerdaten, die mit SAP Benutzerkonten verbunden sind, abgebildet werden sollen.	34976

Tabelle 8: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Bei der Zuordnung einer Active Directory Gruppe zu einem Regal werden unter Umständen mehrere Produktknoten erzeugt.	34552
Wenn in einer Entscheidungsebene mit mehreren Entscheidungsschritten einer der Schritte eskaliert wird, dann wird in der Attestierungshistorie mitunter der falsche Entscheidungsschritt als eskaliert angezeigt.	34570
Bei der Verlängerung oder Abbestellung einer zeitlich begrenzten Bestellung wird der Zeitpunkt, zu dem ein Produkt abbestellt werden soll, nicht korrekt in UTC Zeit ermittelt.	34619
Personen, die Entscheidungen zu Attestierungsvorgängen an eine andere Person delegiert haben, werden trotzdem informiert, dass Attestierungsvorgänge zur Entscheidung vorliegen.	34695
Der Objektschlüssel für eine Bestellposition (`ShoppingCartItem.ObjectKeyOrdered`) wird unter Umständen nicht korrekt befüllt.	34801
An Entscheidungsschritten für kundenspezifische Entscheidungsmethoden ist keine Auswahl einer Rolle (`ObjectKeyOfAssignedOrg`) möglich.	34805
Beim Umzug mehrerer Produkte, für die Bestellungen existieren, in ein anderes Regal, werden manche Bestellungen abgebrochen, obwohl für alle Leistungspositionen **Bestellung bleibt bei Umzug bestehen** aktiviert ist.	34914
Mitgliedschaften in Geschäftsrollen können bestellt werden, auch wenn die zugehörige Leistungsposition als nicht bestellbar gekennzeichnet ist.	34934
Der Analyzer beachtet die Programmfunktion **ApplicationStart_Analyzer** nicht.	34935
Automatische Entscheidungen per `ReuseDecision` bleiben unter Umständen in einer Endlosschleife hängen.	35003
Schreibfehler in den Mailvorlagen **IT Shop- Entscheidungen per E-Mail**	35029

Gelöstes Problem	Fehler ID
und **Attestierung - Entscheidung per E-Mail**.	
Performanceprobleme bei der Neuberechnung der Entscheider im IT Shop.	35117, 35302, 35357
Bei Zuweisungsbestellungen wird der Objektschlüssel der Zuweisung nicht ermittelt, wenn der Objektschlüssel des bestellten Produkts nicht vorhanden ist.	35121
Performanceprobleme bei der Berechnung von Unternehmensrichtlinien, wenn eine große Menge an Objekten betroffen ist.	35139
Die Konsistenzprüfung **Objectkey references to non existing object** erkennt Bestellpositionen für Zuweisungsbestellungen als fehlerhaft.	35143
Fehler bei der Erzeugung des Berichts für das Attestierungsobjekt im Attestierungsvorgang, wenn das Attestierungsobjekt sehr viele rekursiv erreichbare, abhängige Objekte hat.	35254
Der Bericht **Übersicht mit Rollen und Benutzerkonten (inklusive Historie)** ist unvollständig.	35366
Wird ein Entscheidungsschritt aufgrund eines Timeouts automatisch abgelehnt, wird unter Umständen der nachfolgende Entscheidungsschritt nicht ausgeführt.	35440, 35454
Bei der Neuberechnung der Zuweisungen von SAP Rollen an Benutzerkonten wird ein falsches Gültigkeitsdatum ermittelt, wenn die Zuweisung durch eine Zuweisungsbestellung entstanden ist und der Besteller gelöscht wurde.	35434

Siehe auch:

- Schemaänderungen auf Seite 29
- Patches für Synchronisationsprojekte auf Seite 32

Bekannte Probleme

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

Tabelle 9: Allgemein

Bekanntes Problem	Fehler ID
Fehler im Report Editor, wenn im Bericht Spalten verwendet werden, die im	23521

Bekanntes Problem	Fehler ID
Report Editor als Schlüsselworte definiert sind. Workaround: Erstellen Sie Datenabfragen als SQL-Abfragen und nutzen Sie für die betroffenen Spalten Aliasnamen.	
Wird der Web Installer gleichzeitig in mehreren Instanzen gestartet, kann es zu Zugriffsfehlern kommen.	24198
Header-Zeilen in als CSV gespeicherten Reporten enthalten keine sprechenden Namen.	24657
Nach einer Simulation im Manager sind Objekte unter Umständen im inkonsistentem Zustand. Wird ein Objekt während einer Simulation verändert, gespeichert und die Simulation beendet, so bleibt das Objekt im letzten Zustand der Simulation erhalten. Weitere Änderungen an dieser Objektinstanz können unter Umständen nicht gespeichert werden. Lösung: Laden Sie nach dem Beenden der Simulation das Objekt neu.	12753
Im Configuration Wizard können unzulässige Modulkombinationen ausgewählt werden. Dies führt erst bei Beginn der Schemainstallation zu Fehlern. Ursache: Der Configuration Wizard wurde direkt gestartet. Lösung: Verwenden Sie zur Installation der One Identity Manager Komponenten immer die `autorun.exe`. Damit ist sichergestellt, das keine unzulässigen Modulkombinationen ausgewählt werden.	25315
Schemaerweiterungen an einer Datenbanksicht vom Typ **View** (beispielsweise `Department`) mit einer Fremdschlüsselbeziehung auf eine Spalte einer Basistabelle (beispielsweise `BaseTree`) oder einer Datenbanksicht vom Typ **View** sind nicht zulässig.	27203
Fehler bei der Verbindung über einen Anwendungsserver, wenn der private Schlüssel des Zertifikates, mit dem die `VI.DB` ihre Session-Information zu 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.	29535

Bekanntes Problem	Fehler ID
Zur Überprüfung des Schemas wird eine Konsistenzprüfung **Table of type U or R with wrong PK definition** bereitgestellt.	
Wenn die One Identity Manager-Datenbank in einem SQL-Cluster (High Availibility Group) installiert ist und die Option `DTC_SUPPORT = PER_DB` gesetzt ist, erfolgt die Replikation zwischen den Servern mittels Distributed Transaction. Falls dabei ein `Save Transaction` ausgeführt wird, tritt ein Fehler auf: `Cannot use SAVE TRANSACTION within a distributed transaction.` Lösung: Deaktivieren Sie die Option `DTC_SUPPORT = PER_DB`.	30972
Ist explizit kein Datum angegeben, wird intern das Datum 30.12.1899 verwendet. Dies ist bei Wertevergleichen zu beachten, beispielsweise bei der Verwendung in Berichten. Ausführliche Informationen zur Verwendung von Datumsangaben in Berichten finden Sie im *One Identity Manager Konfigurationshandbuch*.	31322
Bei der Installation der Datenbank unter SQL Server 2019 tritt ein Fehler auf: `QBM_PDBQueueProcess_Main unlimited is only allowed as an agent job` Lösung: • Das kumulative Update 2 für SQL Server 2019 wird nicht unterstützt. Weitere Informationen finden Sie unter https://support.oneidentity.com/kb/315001.	32814

Tabelle 10: Webanwendungen

Bekanntes Problem	Fehler ID
Bei der Installation des Web Portals mit dem Web Installer kann folgende Fehlermeldung auftreten: `Diese Zugriffssteuerungsliste liegt nicht in der kanonischen Form vor und kann aus diesem Grund nicht geändert werden.` Der Fehler tritt oft nach einem Windows 10 Anniversary Update auf. Lösung: Ändern Sie auf dem Elternordner der Webanwendung (standardmäßig `C:\inetpub\wwwroot`) die Berechtigungen für den Benutzer und wenden Sie diese Änderung an. Nehmen Sie anschließend diese Änderung wieder zurück.	26739
Die Bestelleigenschaften eines Produktes werden bei der Verlängerung oder Abbestellung im Web Portal nicht aus der ursprünglichen Bestellung in den Warenkorb übernommen. Ursache: Bestelleigenschaften können in unterschiedlichen, kundenspezifischen Spalten gespeichert werden. Lösung: Erstellen Sie eine Bildungsregel für die (kundenspezifische) Spalte	32364

Bekanntes Problem	Fehler ID
an der Tabelle `ShoppingCartItem`, in der die Bestelleigenschaft bei der Bestellung gespeichert wird. Diese Bildungsregel muss die Bestel-leigenschaften für die verknüpfte Bestellung aus der identischen (kunden-spezifischen) Spalte an der Tabelle `PersonWantsOrg` auslesen.	
Es ist nicht möglich mithilfe des Web Designer in der Kopfzeile neben dem Firmennamen/-logo einen Link im Web Portal zu platzieren.	32830
Es ist möglich im Web Portal einen Bericht zu abonnieren, ohne dabei einen Zeitplan auszuwählen. Workarounds: • Erstellen Sie eine Erweiterung auf das entsprechende Formular, mit der unter der Auswahlliste ein Hinweistext angezeigt wird, der auf das Problem hinweist. • Legen Sie einen Standard-Zeitplan für abonnierbare Berichte fest. • Ändern Sie im Web Designer den Konfigurationsschlüssel **Filter für abonnierbare Berichte** (**VI_Reporting_Subscription_FilterRPSSubscription**) und setzen Sie den Wert von **Minimale Anzahl Zeichen** des Zeitplans (`UID_DialogSchedule`) auf **1**.	32938

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

Im Web Portal werden in der Detailanzeige eines offenen	34110

Bekanntes Problem	Fehler ID
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.	

Tabelle 11: Zielsystemanbindung

Bekanntes Problem	Fehler ID
Bei Windows PowerShell Verbindungen, welche intern `Import-PSSession` verwenden, kommt es zu Speicherlecks.	23795
Der Baustein **HR_ENTRY_DATE** eines SAP HCM Systems ist standardmäßig nicht remote aufrufbar. Lösung: Ermöglichen Sie den Remotezugriff auf den Baustein **HR_ENTRY_DATE** in Ihrem SAP HCM System. Erstellen Sie im Synchronization Editor das Mapping für die Schemaeigenschaft `EntryDate`.	25401
Beim Anlegen von Microsoft Exchange Postfächern werden gegebenenfalls vorhandene sekundäre SIP-Adressen in primäre SIP-Adressen umgewandelt, sofern bisher keine primären SIP-Adressen hinterlegt waren.	27042
Fehler im Domino Konnektor (`Error getting revision of schema type ((Server))`). Wahrscheinliche Ursache: Die HCL Domino-Umgebung wurde neu aufgebaut oder es wurden zahlreiche Einträge in das Domino-Verzeichnis eingefügt. Lösung: Aktualisieren Sie in der HCL Domino-Umgebung die Indexe im Domino-Verzeichnis manuell.	27126
Der SAP Konnektor stellt keine Schemaeigenschaft bereit, um zu erkennen, ob ein Benutzer in der SAP R/3-Umgebung ein produktives Kennwort hat. Wenn diese Information im One Identity Manager zur Verfügung stehen soll, erweitern Sie das Schema und die Synchronisationskonfiguration. • Legen Sie eine kundenspezifische Spalte an der Tabelle `SAPUser` an. • Erweitern Sie im Synchronisationsprojekt das SAP Schema um einen neuen Schematyp, der die benötigte Information liefert. • Passen Sie die Synchronisationskonfiguration an.	27359
Synchronisationsprojekte für SAP R/3, die per Transport in eine One Identity Manager Datenbank importiert wurden, können nicht geöffnet werden. Das Problem tritt nur auf, wenn vor dem Import des	27687

Bekanntes Problem	Fehler ID
Transportpakets noch kein SAP R/3 Synchronisationsprojekt in der Zieldatenbank angelegt wurde. Lösung: Erstellen und speichern Sie mindestens ein Synchronisationsprojekt für SAP R/3 in der Zieldatenbank, bevor Sie SAP R/3 Synchronisationsprojekte mit dem Database Transporter in diese Datenbank importieren.	
Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer Zentralen Benutzerverwaltung. Meldung: `No company is assigned.` Ursache: Für das Benutzerkonto konnte keine Firmenadresse ermittelt werden. Lösung: Stellen Sie sicher, dass entweder • jedem Benutzerkonto eine Firma zugeordnet ist, die im Zentralsystem existiert - ODER - • dem Zentralsystem eine Firma zugeordnet ist.	29253
Bei der Synchronisation von SAP R/3 Personalplanungsdaten, die erst zukünftig wirksam werden, werden einige Daten nicht eingelesen. Ursache: Die Funktion `BAPI_EMPLOYEE_GETDATA` wird immer mit dem aktuellen Tagesdatum ausgeführt. Damit werden Änderungen taggenau beachtet. Lösung: Für eine Vorab-Synchronisation von Personaldaten, die erst zukünftig wirksam werden, nutzen Sie eine Schemaerweiterung und lesen Sie die Daten aus der Tabelle `PA0001` direkt ein.	29556
Der Zielsystemabgleich zeigt in der Manager Webanwendung keine Informationen an. 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	31017

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

Wenn Datumsfelder in einer SAP R/3-Umgebung Werte enthalten, die kein gültiges Datums- oder Uhrzeitformat repräsentieren, kann der SAP Konnektor diese Werte nicht lesen, da die Typkonvertierung scheitert.
Lösung: Bereinigen Sie die fehlerhaften Daten.
Workaround: Die Typkonvertierung kann deaktiviert werden. Voraussetzung dafür ist, dass auf dem Synchronisationsserver der SAP .Net Connector for .NET 4.0 on x64, mindestens Version 3.0.15.0 installiert ist.
WICHTIG: Da mit diesem Workaround die Datumsprüfung komplett umgangen wird, sollte er nur genutzt werden, wenn keine andere Lösung umsetzbar ist.
Um die Typkonvertierung zu deaktivieren
• Fügen Sie folgende Einstellungen in die Datei `StdioProcessor.exe.config` ein.
• In die vorhandene Sektion `<configSections>`:
`<sectionGroup name="SAP.Middleware.Connector">`
`<section name="GeneralSettings" type="SAP.Middleware.Connector.RfcGeneralConfiguration, sapnco, Version=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c7f7d23" />`
`</sectionGroup>`
• Eine neue Sektion:
	32149

Bekanntes Problem	Fehler ID
<SAP.Middleware.Connector> <GeneralSettings anyDateTimeValueAllowed="true" /> </SAP.Middleware.Connector>	
Die in der Prozesskomponente PowershellComponentNet4 im Parameter OutputFile zu erzeugende Datei enthält keine Fehlermeldungen. Ursache: In der Datei (Parameter OutputFile) werden keine Meldungen gesammelt. Die Datei dient als Exportdatei der in der Pipeline zurückgelieferten Objekte. Lösung: Die Ausgabe von Meldungen im Skript kann mittels *> Operator in eine im Skript festgelegte Datei erfolgen. Beispiel: Write-Warning "Ich bin eine Meldung" *> "meldungen.txt" Weiterhin werden Meldungen, die Mittels Write-Warning generiert werden, ebenfalls in die Protokolldatei des One Identity Manager Service geschrieben. Möchte man einen Abbruch mit Fehler im Skript erzwingen, so sollte man eine Exception werfen. Diese Meldung erscheint dann in der Protokolldatei des One Identity Manager Service.	32945
Der Google Workspace Konnektor kann die Nutzerdaten von Google Applikationen vor dem Löschen eines Benutzerkontos nicht erfolgreich auf ein anderes Google Workspace Benutzerkonto übertragen. Der Transfer scheitert an den Nutzerdaten der Applikation Rocket. Workaround: Hinterlegen Sie in den erweiterten Einstellungen der Systemverbindung zur Google Workspace ein Nutzerdatentransfer XML. In diesem XML-Dokument schränken Sie die Liste der zu übertragenden Nutzerdaten ein. Führen Sie nur die Google Applikationen auf, deren Nutzerdaten Sie weiterhin benötigen. Ausführliche Informationen und ein Beispiel-XML finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Google Workspace-Umgebung*.	33104
Wenn in der Schematypdefinition einer Schemaerweiterungsdatei für das SAP R/3-Schema ein DisplayPattern definiert ist und darin Spalten verwendet werden, die im SAP R/3-Schema einen anderen Namen haben als im One Identity Manager Schema, können Performanceprobleme auftreten. Lösung: Lassen Sie DisplayPattern in der Schematypdefinition leer. Es wird automatisch der definierte Name des Objekts als Anzeigewert verwendet.	33812
Enthalten Zielsystemdaten nachgestellte Leerzeichen so gehen diese bei der Synchronisation in den One Identity Manager verloren. Jede weitere Synchronisation erkennt Datenänderungen und schreibt die betroffenen	33448

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

Tabelle 12: Identity Management und Access Governance

Bekanntes Problem	Fehler ID
Bei der Genehmigung einer Bestellung mit Selbstbedienung wird das Ereignis `Granted` für den Entscheidungsschritt nicht ausgelöst. In kundenspezifischen Prozessen kann stattdessen das Ereignis `OrderGranted` genutzt werden.	31997
Wenn eine Zuweisung über die Rollenhierarchie vererbt wird, wird an der geerbten Zuweisung das **Bit 1** gesetzt. Geerbte Zuweisungen sind folglich immer indirekt zugewiesen, auch wenn sie ursprünglich direkt, über eine dynamische Rolle oder eine Zuweisungsbestellung entstanden sind.	35193

Tabelle 13: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
Unter SharePoint 2010 kann es zu einem Fehler bei der Synchronisation von SharePoint Websites kommen. Die Methode `SPWeb.FirstUniqueRoleDefinitionWeb()` löst eine `ArgumentException` aus. Weitere Informationen finden Sie unter https://support.microsoft.com/de-de/kb/2863929.	24626
Die Installation des One Identity Manager Service mit Server Installer auf einem Windows Server funktioniert nicht, wenn die Einstellung **File and Printer Sharing** am Server deaktiviert ist. Auf einem Domänen-Controller ist diese Einstellung aus Sicherheitsgründen deaktiviert.	24784
Beim Verbinden mit einer Oracle Database kommt es sporadisch zu einem der folgenden Fehler: TNS-12516, TNS-12519 oder ORA-12520. Erneute Verbindungsversuche sind jedoch meist erfolgreich. Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am	27830

Bekanntes Problem	Fehler ID
Server konfigurierte Limit.	
In einem mehrseitigen Synchronisationsprotokoll kann nicht mit der Maus und mit den Pfeiltasten navigiert werden. Ursache: Die StimulReport.Net-Komponente der Firma Stimulsoft behandelt den Bericht als eine Seite.	29051
Gültiger CSS-Code verursacht einen Fehler unter Mono, wenn doppelte Schlüssel vorhanden sind. Weitere Informationen finden Sie unter https://github.com/mono/mono/issues/7455.	762534, 762548, 29607
Mitgliedschaften in Active Directory Gruppen vom Typ **Universal** in einer untergeordneten Domäne werden im Zielsystem nicht entfernt, wenn eines der folgenden Windows Updates installiert ist: • Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 Uns ist derzeit nicht bekannt, ob weitere Windows Updates zu diesem Fehler führen können. Der Active Directory Konnektor korrigiert dieses Fehlverhalten mit einem Workaround beim Aktualisieren der Mitgliederliste. Da dieser Workaround die Performance bei der Provisionierung von Active Directory Gruppen verschlechtern kann, wird er aus künftigen One Identity Manager Versionen wieder entfernt, sobald Microsoft diesen Fehler behoben hat.	30575
Unter Umständen kommt es im Report Editor zur Verwendung der falschen Sprache in den Steuerelementen von Stimulsoft.	31155
Bei der Anbindung eines externen Webservices über den Webservice-Integrationsassistenten stellt der Webservice die Daten über eine `WSDL`-Datei bereit. Mittels des WSDL-Tools von Microsoft werden diese Daten in Visual Basic .NET Code umgewandelt. Wenn im so generierten Code Standard-Datentypen überschrieben werden (beispielsweise wenn nochmals der Datentyp `boolean` definiert wird), kann das im One Identity Manager zu verschiedenen Problemen führen.	31998

In bestimmten Active Directory/Microsoft Exchange-Topologien schlägt das Cmdlet `Set-Mailbox` mit folgendem Fehler fehl:
`Error on proxy command 'Set-Mailbox...'`
`The operation couldn't be performed because object '...' couldn't be found on '...'.`
Weitere Informationen finden Sie unter https://support.microsoft.com/en-us/help/4295103.
Mögliche Workarounds:
	33026

- 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.

Schemaänderungen

Nachfolgend finden Sie eine Übersicht der Schemaänderungen von Version 8.2 zu Version 8.2.1.

Konfigurationsmodul

- Neue Tabellen `QBMAdaptiveCard` und `QBMAdaptiveCardTemplate` für die Integration mit Starling Cloud Assistant.

Modul Zielsystemsynchronisation

- Neue Tabelle `DPRProjectionObjectState` zur Abbildung von Objektreferenzen für die Synchronisation.
- Neue Spalte `DPRJournal.CompletionTime` zur Abbildung des Zeitpunktes, an dem die Synchronisation beendet wurde.
- Neue Spalte `DPRSystemMappingRule.ConcurrenceBehavior` zur Abbildung des Verhaltens bei gleichzeitiger Datenänderung.
- Neue Spalte `DPRSystemMappingRule.DisableMergeModeSupport` zum Deaktivieren des Mergemodus.

Zielsystem Basismodul

- Neue Tabellen für die Ermittlung eines Änderungsdatum für Gruppen inklusive ihrer Mitgliedschaften.
  - TSBVUNSGroupRevision
  - TSBVUNSGroupBRevision

- TSBVUNSGroupB1Revision
- TSBVUNSGroupB2Revision
- TSBVUNSGroupB3Revision
- TSBVUNSAccountBRevision

Azure Active Directory Modul

- Neue Spalte `AADGroup.HasReadOnlyMemberships` zur Abbildung von dynamischen Mitgliedschaften.

Exchange Online Modul

- Neue Spalten `O3EMailUser-RecipientTypeDetails` und `O3EMailUser.RecipientType` zur besseren Abbildung des Empfängertyps eines E-Mail Benutzers.

Identity Management Basismodul

- Neue Spalten `QERWorkingStep.ApproveReasonType` und `QERWorkingStep.DenyReasonType` zur Abbildung der Art der Begründung.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 8.2 zu Version 8.2.1. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 65.

Änderungen an Synchronisationsvorlagen

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen. Um Änderungen an Synchronisationsvorlagen in bestehende Synchronisationsprojekte zu übernehmen, werden Patches bereitgestellt. Weitere Informationen finden Sie unter Patches für Synchronisationsprojekte auf Seite 32.

Tabelle 14: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Azure Active Directory Modul	Azure Active Directory Synchronization	geändert

Modul	Synchronisationsvorlage	Art der Änderung
Active Directory Modul	Active Directory Synchronization	keine
Active Roles Modul	Synchronize Active Directory Domain via Active Roles	keine
Modul Cloud Systems Management	Universal Cloud Interface synchronization	keine
Oracle E-Business Suite Modul	Oracle E-Business Suite Synchronization	geändert
	Oracle E-Business Suite CRM data	geändert
	Oracle E-Business Suite HR data	geändert
	Oracle E-Business Suite OIM data	geändert
Microsoft Exchange Modul	Microsoft Exchange 2013_2016 Synchronization (v2)	geändert
	Microsoft Exchange 2013 / 2016 Synchronization (abgekündigt)	keine
	Microsoft Exchange 2010 Synchronization (v2)	geändert
Google Workspace Modul	Google Workspace Synchronization	geändert
LDAP Modul	AD LDS Synchronization	geändert
	AD LDS Synchronization (version 2)	geändert
	OpenDJ Synchronization	geändert
	OpenDJ Synchronization (version 2)	geändert
	Generic LDAP Synchronization (version 2)	geändert
	Oracle DSEE Synchronization (version 2)	geändert
Domino Modul	Lotus Domino synchronization	keine
Exchange Online Modul	Exchange Online Synchronization (v2)	geändert
Privileged Account Governance Modul	One Identity Safeguard Synchronization	geändert
SAP R/3 Benutzermanagement-Modul	SAP R/3 Synchronization (Base Administration)	geändert
	SAP R/3 (CUA subsystem)	keine
Modul SAP R/3 Analyseberechtigungen Add-on	SAP R/3 BW	keine

Modul	Synchronisationsvorlage	Art der Änderung
Modul SAP R/3 Compliance Add-on	SAP R/3 authorization objects	keine
Modul SAP R/3 Strukturelle Profile Add-on	SAP R/3 HCM authentication objects	geändert
	SAP R/3 HCM employee objects	geändert
SharePoint Modul	SharePoint Synchronization	geändert
SharePoint Online Modul	SharePoint Online Synchronization	geändert
Modul Universal Cloud Interface	SCIM Connect via One Identity Starling Connect	keine
	SCIM Synchronization	keine
Modul Unix-basierte Zielsysteme	Unix Account Management	geändert
	AIX Account Management	geändert
Modul Zielsys-temsynchronisation	Automatic One Identity Manager synchronization	keine

Patches für Synchronisationsprojekte

Nachfolgend finden Sie eine Liste aller Patches für Synchronisationsprojekte, die im One Identity Manager 8.2.1 bereitgestellt werden. Jeder Patch enthält ein Skript, welches prüft, ob der Patch auf das Synchronisationsprojekt angewendet werden kann. Ob ein Patch angewendet werden kann, ist abhängig von der konkreten Synchronisationskonfiguration.

Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 65.

Tabelle 15: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34896	Verbessertes Mapping von Benutzerkonten in Verbund-Umgebungen	Ändert das Mapping `User`, um die Neuanlage von Azure Active Directory Benutzerkonten zu unterstützen, die später mit dem verbundenen Active Directory Benutzerkonto synchronisiert werden. Bei Benutzerkonten, für welche die Synchronisation mit dem lokalen Active Directory aktiviert ist (`OnPremisesSyncEnabled = True`), werden bestimmte Schemaeigenschaften nur gelesen.	34896

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

Tabelle 16: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34775	Anlegen einer Kennwort-Variable	Legt eine Variable für das Kennwort des Synchronisationsbenutzers an und ersetzt das Kennwort im Verbindungsparameter durch diese Variable. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34775

Tabelle 17: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#21073_2	Verwalten von Postfachberechtigungen (2)	Lässt nur solche Prinzipale zu, die auch im Exchange Admin Center verfügbar sind. Abhängig von Patch **Unterstützung der Postfachberechtigungen Senden als und Vollzugriff**. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	21073
VPR#35343_EX0	Ändern des Verhaltens von "unbegrenzten" Werten	Änderung des Verhaltens von "unbegrenzten" Werten. Sie werden in der Datenbank als -1 anstelle von 0 dargestellt, wodurch tatsächliche 0-Werte behandelt werden können. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35343

Tabelle 18: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34938	Neue Property-Mapping-Regeln für den Empfängertyp von E-Mail Benutzern	Fügt zwei Property-Mapping-Regeln für den Empfängertyp in das Mapping `MailUser` ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34938
VPR#35373	Korrektur falscher Verarbeitungsmethoden in Synchronisationsworkflows	Entfernt falsch festgelegte Verarbeitungsmethoden aus den Synchronisationsschritten **Calendar Processing** und **Mailbox Statistics** aus den Workflows. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35373
VPR#35343_O3E	Ändern des Verhaltens von "unbegrenzten" Werten	Änderung des Verhaltens von "unbegrenzten" Werten. Sie werden in der Datenbank als -1 anstelle von 0 dargestellt, wodurch tatsächliche 0-Werte behandelt werden können.	35343

Tabelle 19: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35118	Neue Property-Mapping-Regeln für das Mapping von ALE Modelname und ALE Name	Fügt Property-Mapping-Regeln zum Einlesen des ALE Modelnamen und des ALE Namen aus dem Zentralsystem einer ZBV in das Mapping `aLEModel` ein.	35118
VPR#35370	Korrektur des Referenzscopes	Korrigiert den Referenzscope der One Identity Manager-Verbindung für die korrekte Abbildung von Stellvertretern an SAP Benutzerkonten. Voraussetzung für Patch **Korrektur**	35370

Patch ID	Patch	Beschreibung	Fehler ID
		des Referenzscopes (für ZBV). Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	
VPR#35370_CUA	Korrektur des Referenzscopes (für ZBV)	Korrigiert den Referenzscope der One Identity Manager-Verbindung für die korrekte Abbildung von Stellvertretern an SAP Benutzerkonten im Zentralsystem einer ZBV. Abhängig von Patch **Korrektur des Referenzscopes**. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35370

Tabelle 20: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35174_1	Aktualisierung von `SAPUserInSAPHRP` bei der Provisionierung zulassen (Teil 1/2)	Korrigiert den Provisionierungsworkflow, um die Aktualisierung von Zuweisungen struktureller Profile an Benutzerkonten zu ermöglichen. Voraussetzung für Patch **Aktualisierung struktureller Profile bei der Provisionierung (Teil 2/2)**. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35174
VPR#35174_2	Aktualisierung von `SAPUserInSAPHRP` bei der Provisionierung zulassen (Teil 2/2)	Korrigiert die Synchronisationskonfiguration, um die Aktualisierung von Zuweisungen struktureller Profile an Benutzerkonten zu ermöglichen. Abhängig von Patch **Aktualisierung struktureller Profile bei der Provisionierung (Teil 1/2)**. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	35174

Patches in One Identity Manager Version 8.2

Tabelle 21: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2.1	Meilenstein für den Kontext **DPR**".	
	Meilenstein 8.2.1	Meilenstein für den Kontext **One Identity Manager**.	

Tabelle 22: Patches für Azure Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#28669	Unterstützung von Einladungen von Gastbenutzern	Erweitert das Mapping `User` für die Erstellung von Gastbenutzern durch das Versenden von Einladungen.	28669
VPR#31389	Unterstützung von Schemaeigenschaften für Hybrid-Umgebungen, Altersgruppen und Benutzerprofilen	Fügt neue Property-Mapping-Regeln in das Mapping `User` ein, zur Unterstützung von Hybrid-Umgebungen, Altersgruppen und Benutzerprofilen.	31389
VPR#32384	Unterstützung von Lizenzzuweisungen über Azure Active Directory Gruppen	Erweitert die Synchronisationskonfiguration zur Unterstützung von Lizenzzuweisungen über Azure Active Directory Gruppen.	32384
VPR#32454	Setzt das Schlagwort **AzureAD** an Synchronisationsprojekten	Setzt das Schlagwort **AzureAD** an Synchronisationsprojekten für Azure Active Directory.	32454
VPR#32665	Synchronisation von `ExternalUserState` und `ExternalUserStateChangeDateTime`	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `ExternalUserState` und `ExternalUserStateChangeDateTime` in das Mapping `User` ein.	32665
VPR#32975	Hinzufügen einer Property-Mapping-Regel für `LastPasswordChangeDateTime`	Fügt eine Property-Mapping-Regel für `LastPasswordChangeDateTime` in das Mapping `User` ein.	32975
VPR#33088	Unterstützung für Azure Active Directory Dienstprinzipale	Erweitert die Synchronisationskonfiguration zur Unterstützung von Azure Active Directory Dienst-	33088

Patch ID	Patch	Beschreibung	Fehler ID
		prinzipalen und App-Rollen. Voraussetzung für Patch **Unterstützung von Active Directory Richtlinien**.	
VPR#33198	Unterstützung von Active Directory Richtlinien	Erweitert die Synchronisationskonfiguration zur Unterstützung von Active Directory Richtlinien. Abhängig von Patch **Unterstützung für Azure Active Directory Dienstprinzipale**.	33198
VPR#34150	Unterstützung von Microsoft Cloud for US Government (L4)	Fügt die Unterstützung für Microsoft Cloud for US Government (L4) ein.	34150
	Meilenstein 8.2.1	Meilenstein für den Kontext **Azure Active Directory**.	

Tabelle 23: Patches für Active Directory

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32110	Hinzufügen der Schemaeigenschaft `middleName`	Fügt die Schemaeigenschaft `middleName` in die Mappings `user` und `inetOrgPerson` ein.	32110
VPR#32759	Hinzufügen von Property-Mapping-Regeln für die Schemaeigenschaft `ProtectedFromAccidentalDeletion`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `ProtectedFromAccidentalDeletion` in die Mappings `user`, `contact`, `group` und `computer` ein.	32759
VPR#32950	Hinzufügen weiterer Property-Mapping-Regeln für die Schemaeigenschaft `mS-DS-ConsistencyGuid`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `mS-DS-ConsistencyGuid` in die Mappings `contact`, `group` und `computer` ein. Voraussetzung für Patch **Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft `mS-DS-ConsistencyGuid`**.	32950

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33217_001	Prüft die Eigenschaften von Mappings	Prüft und korrigiert Mappings, bei denen die Option **Nicht für Neuanlage geeignet** aktiviert ist.	33217
VPR#34324	Publizieren der Gruppenmitglieder als schreibgeschützt	Publizieren der Eigenschaften `member` von Gruppen als schreibgeschützt, um Schreibvorgänge im Zielsystembrowser zu vermeiden.	34324
VPR#34715	Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft `mS-DS-ConsistencyGuid`	Korrigiert die Mappingrichtung der Property-Mapping-Regel für die Schemaeigenschaft `mS-DS-ConsistencyGuid` im Mapping `user`. Abhängig von Patch **Hinzufügen weiterer Property-Mapping-Regeln für die Schemaeigenschaft `mS-DS-ConsistencyGuid`**.	34715
	Meilenstein 8.2.1	Meilenstein für den Kontext **Active Directory**.	

Tabelle 24: Patches für Active Roles

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32110	Neue Property-Mapping-Regel für `middleName`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `middleName` in die Mappings `User` und `InetOrgPerson` ein.	32110
VPR#32783	Neue Property-Mapping-Regel für `edsvaProtectFromDeletion`	Fügt eine Property-Mapping-Regel für `edsvaProtectFromDeletion` in die Mappings `Group`, `Computer`, `User` und `InetOrgPerson` ein.	32783
VPR#32952	Hinzufügen von Property-Mapping-Regeln für `mS-DS-ConsistencyGuid`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `mS-DS-`	32952

Patch ID	Patch	Beschreibung	Fehler ID
		ConsistencyGuid in die Mappings Contact, Group, Computer, User und InetOrgPerson ein.	
VPR#34168	Neue Property-Mapping-Regel für edsaIsDynamicGoup	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft edsaIsDynamicGoup in das Mapping Group ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34168
VPR#34634	Neue Property-Mapping-Regeln für edsvaGFIsGroupFamily und edsvaCGIsControlledGroup	Fügt Property-Mapping-Regeln für die Schemaeigenschaften edsvaGFIsGroupFamily und edsvaCGIsControlledGroup in das Mapping Group ein.	34634
	Meilenstein 8.2.1	Meilenstein für den Kontext **Active Roles**.	

Tabelle 25: Patches für Oracle E-Business Suite

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33804	Bereinigung von Verbindungsparametern	Entfernt nicht benötigte Parameter der Systemverbindung aus dem Verbindungsparameter. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	33804
	Meilenstein 8.2.1	Meilenstein für den Kontext **Oracle E-Business Suite**.	

Tabelle 26: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#21073	Unterstützung der Postfachberechtigungen **Senden als** und **Vollzugriff**	Erweitert die Synchronisationskonfiguration zur Unterstützung der	21073

Patch ID	Patch	Beschreibung	Fehler ID
		Postfachberechtigungen **Senden als** und **Vollzugriff**. HINWEIS: Da dies große Auswirkungen auf die Performance hat, sind die entsprechenden Synchronisationsschritte standardmäßig deaktiviert und müssen manuell aktiviert werden.	
VPR#26120	Neue Property-Mapping-Regeln für `IsExcludedFromProvisioning` und `IsSuspendedFromProvisioning`	Fügt Property-Mapping-Regeln für die Schemaeigenschaften `IsExcludedFromProvisioning` und `IsSuspendedFromProvisioning` in das Mapping `MailboxDatabase` ein.	26120
VPR#27741	Unterstützung von Adressbuchrichtlinien	Erweitert die Synchronisationskonfiguration zur Unterstützung von Adressbuchrichtlinien für Postfächer.	27741
VPR#31470	Neue Property-Mapping-Regel für `IsSingleItemRecoveryEnabled`	Fügt eine Property-Mapping-Regel für die Schemaeigenschaft `IsSingleItemRecoveryEnabled` in das Mapping `Mailbox` ein.	31470
	Meilenstein 8.2.1	Meilenstein für den Kontext **Microsoft Exchange**.	

Tabelle 27: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#34170	Unterstützung von Microsoft Cloud for US Government (L4)	Fügt die Unterstützung für Microsoft Cloud for US Government (L4) ein. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34170
VPR#34046	Neue Property-	Fügt eine Property-Mapping-Regel	34046

Patch ID	Patch	Beschreibung	Fehler ID
	Mapping-Regel für `HiddenFromExchange-ClientsEnabled`	für die Schemaeigenschaft `HiddenFromExchange-ClientsEnabled` im Mapping `UnifiedGroup` ein.	
	Meilenstein 8.2.1	Meilenstein für den Kontext **Exchange Online**.	

Tabelle 28: Patches für Google Workspace

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32610	Abbildung verschiedener Zugriffsberechtigungen von Gruppen	Erweitert das Mapping `Group` zur Abbildung von Zugriffsberechtigungen. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	32610
VPR#33093	Abbildung zusätzlicher Schemaeigenschaften für Benutzerkonten	Erweitert das Mapping `User` zur Abbildung weiterer Schemaeigenschaften von Benutzerkonten.	33093
VPR#34645	Korrektur im Mapping `User`	Korrigiert die Property-Mapping-Regel für die Schemaeigenschaft `Aliases` im Mapping `User`.	34645
	Meilenstein 8.2.1	Meilenstein für den Kontext **Google Workspace**.	

Tabelle 29: Patches für LDAP

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33513	Unterstützung mehrerer Domänen mit dem gleichen DN	Erweitert den Scope und das Standardvariablenset, um mehrere Domänen mit dem gleichen definierten Namen zu unterstützen.	33513
	Meilenstein 8.2.1	Meilenstein für den Kontext **LDAP**.	

Tabelle 30: Patches für HCL Domino

Patch ID	Patch	Beschreibung	Fehler ID
VPR#25230	Ändert den Standardwert der Variable `MailFileAccessType`	Ändert den Standardwert der Variable `MailFileAccessType` auf **0**.	25230
VPR#34393	Korrektur einer Property-Mapping-Regel im Mapping `Person`	Korrigiert Einstellungen der Property-Mapping-Regel für InternetPassword im Mapping `Person`. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34393
	Meilenstein 8.2.1	Meilenstein für den Kontext **HCL Domino**.	

Tabelle 31: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32541	Unterstützung von Zugriffsanforderungen für SSH-Schlüssel	Fügt Property-Mapping-Regeln in die Mappings `Asset` und `AssetAccount` ein, um Zugriffsanforderungen für SSH-Schlüssel zu unterstützen.	32541
VPR#34392	Unterstützung der Vault für persönliche Kennwörter	Fügt Property-Mapping-Regeln für die Schemaeigenschaft `AllowPersonalAccounts` ins Mapping `User` ein.	34392
VPR#34403	Behandlung von Kennwörtern als geheime Werte	Aktualisiert das Konnektorschema, um Kennwörter als geheime Werte zu behandeln. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	34403
	Meilenstein 8.2.1	Meilenstein für den Kontext **Privileged Account Management**.	

Tabelle 32: Patches für SAP R/3

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33217_002	Prüft die Eigenschaften von Mappings	Prüft und korrigiert Mappings,	33217

Patch ID	Patch	Beschreibung	Fehler ID
		bei denen die Option **Nicht für Neuanlage geeignet** aktiviert ist.	
VPR#33301	Unterstützung von SAP S/4HANA Nutzertypen und Kommunikationsdaten	Erweitert die Synchronisationskonfiguration zur Abbildung der Adress- und Kommunikationsdaten von Geschäftspartnern.	33301
VPR#33301_2	Unterstützung von SAP S/4HANA Nutzertypen	Erweitert die Synchronisationskonfiguration zur Abbildung von Nutzertypen.	33301
VPR#33819	Neu Property-Mapping-Regel für die Standardfirma von SAP Mandanten	Fügt eine Property-Mapping-Regel zur Abbildung der Standardfirma von SAP Mandanten in das Mapping `mandant` ein.	33819
VPR#34563	Korrektur von `userInRole` Mapping und Synchronisationsschritt	Korrigiert das Mapping und den Synchronisationsschritt für `SAPUserInSAPRole`-Zuweisungen, die nicht wirksam sind. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet. Abhängig von Patch **Legt eine Schemaklasse für den Schematyp SAPUserInSAPRole an** (VPR#31427).	34563
	Meilenstein 8.2.1	Meilenstein für den Kontext **SAP R/3**.	

Tabelle 33: Patches für SAP R/3 Personalplanungsdaten und strukturelle Profile

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2.1	Meilenstein für den Kontext **SAP R/3 Strukturelle Profile Add-on**.	

Tabelle 34: Patches für SAP R/3 BI Analyseberechtigungen

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2.1	Meilenstein für den Kontext **SAP R/3 Analyseberechtigungen Add-on**.	

Tabelle 35: Patches für SAP R/3 Berechtigungsobjekte

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

Patch ID	Patch	Beschreibung	Fehler ID
		1).	
	Meilenstein 8.2.1	Meilenstein für den Kontext **SAP R/3**.	

Tabelle 36: Patches für SharePoint

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2.1	Meilenstein für den Kontext **SharePoint**.	

Tabelle 37: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#31779	Konfiguration zum Anlegen und Löschen von Websitesammlungen und Websites	Erweitert die Synchronisationskonfiguration, um Websitesammlungen und Websites anlegen und löschen zu können.	31779
	Meilenstein 8.2.1	Meilenstein für den Kontext **SharePoint Online**.	

Tabelle 38: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
VPR#32564	Konfiguration der Anzahl paralleler Anfragen	Fügt die Variable **Max. Parallel Queries** ins Standardvariablenset ein.	32564
VPR#33884	Konfiguration des Verbindungsparameters `KeepAlive`	Fügt die Variable **HTTP KeepAlive** ins Standardvariablenset ein.	33884
VPR#33978	Neue Variable zum Einstellen einer Standardzeitzone	Fügt eine Variable ins Standardvariablenset und die Verbindungsparameter ein, um eine Standardzeitzone festlegen zu können. Dieser Patch wird während der Aktualisierung des One Identity Manager automatisch angewendet.	33978
	Meilenstein 8.2.1	Meilenstein für den Kontext **SCIM**.	

Tabelle 39: Patches für die Universal Cloud Interface-Schnittstelle (im Modul Cloud Systems Management)

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2.1	Meilenstein für den Kontext **Universal Cloud Interface**.	

Tabelle 40: Patches für Unix

Patch ID	Patch	Beschreibung	Fehler ID
VPR#Patch32500	Korrektur der Variable **Elevation password**	Kennzeichnet die Variable **Elevation password** als geheimen Wert.	32500
VPR#33249	Neue Variablen und Verbindungsparameter zur Authentifizierung mit dem privaten SSH-Schlüssel	Fügt Variablen und Verbindungsparameter zur Authentifizierung mit dem privaten SSH-Schlüssel ein.	33249
	Meilenstein 8.2.1	Meilenstein für den Kontext **Unix**.	

Tabelle 41: Patches für den One Identity Manager Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
VPR#33728	Aktualisierung des One Identity Manager Schemas	Aktualisiert das One Identity Manager Schema, um die Generierung von Synchronisationsprojekten mit dem One Identity Manager Konnektor zu unterstützen.	33728
	Meilenstein 8.2.1	Meilenstein für den Kontext **Datenbank**.	

Tabelle 42: Patches für den CSV-Konnektor

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 8.2.1	Meilenstein für den Kontext **CSV**.	

Abgekündigte Funktionen

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

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

  Verwenden Sie das Kennwortrücksetzungsportal um Kennwörter zu ändern. Kennwortfragen und Kennwortantworten hinterlegen Sie im Web Portal.
- Der Konfigurationsparameter **QER | Person | UseCentralPassword | PermanentStore** wurde gelöscht.
- Der Systembenutzer **viITShop** wurde gelöscht.

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

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

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

- Der generische LDAP Konnektor wird in zukünftigen Versionen nicht mehr unterstützt. Verwenden Sie den neuen LDAP Konnektor **LDAP Konnektor (Version 2)**.
- Der SOAP Web Service wird in zukünftigen Versionen nicht mehr unterstützt.
- Der SPML Webservice wird in zukünftigen Versionen nicht mehr unterstützt.
- Der Microsoft Exchange 2010 Konnektor wird in zukünftigen Versionen nicht mehr unterstützt.
- Der SharePoint 2010 Konnektor wird in zukünftigen Versionen nicht mehr unterstützt.
- Folgende Skripte sind als veraltet gekennzeichnet. Bei der Kompilierung wird eine entsprechende Warnung ausgegeben.
  - VI_GetValueOfObject
  - VID_GetValueOfDialogObject
  - VI_ITDataFromOrg

    - VI_AE_ITDataFromOrg
    - VI_GetOrgUnitFromCertifier
    - TSB_CreateCanonicalNameFromDN
    - VI_ConvertDNToCanonicalName
    - VI_PersonAuto_LDAP
    - VI_PersonAuto_ADS
    - VI_PersonAuto_EBS
    - VI_PersonAuto_Notes
    - VI_PersonAuto_SAP
    - VI_PersonAuto_SharePoint_SPSUser
- Starling Two-Factor Authentication und die Starling 2FA App werden in zukünftigen Versionen nicht mehr unterstützt, da der Dienst Starling Two-Factor Authentication zum 1. November 2022 abgeschaltet wird.
    - Für die Multifaktor-Authentifizierung bei Bestellungen oder Attestierungen gibt es derzeit keinen Ersatz. Dies wird in einer Folgeversion durch die Integration mit OneLogin ergänzt.
    - Für die Entscheidung von Bestellungen und Attestierungsvorgängen nutzen Sie stattdessen die neue Funktionalität der adaptiven Karten mit Starling Cloud Assistant.

      Die Unterstützung der Starling 2FA App für die Entscheidung von Bestellungen ist in der Version 8.2.1 noch enthalten, jedoch inaktiv.

      Um die Funktionalität zur Entscheidung von Bestellungen per Starling 2FA App temporär zu aktivieren

      1. Aktivieren Sie im Designer den Prozess `VI_ESS_PWOHelperPWO approve anywhere`.
      2. Deaktivieren Sie im Designer den Prozess `QER_PWOHelperPWO approve anywhere`.
- Die Eigenschaft **Relevanz für Compliance** für IT Shop Bestellungen (`PWODecisionStep.ComplianceRelevance` und `QERWorkingStep.ComplianceRelevance`) wird in zukünftigen Versionen nicht mehr unterstützt.
- Die Bearbeitung von API-Definitionscode im API Designer wird abgeschafft.

  Im One Identity Manager API-Entwicklungshandbuch wurde eine Anleitung hinzugefügt, wie man XML-basierten API-Definitionscode in eine Plugin-Bibliothek umwandelt.
- Die Kompilierung von HTML-Anwendungen im Database Compiler wird abgeschafft.
- Die Kompilierung der API-DLL im Database Compiler wird abgeschafft.
- Der API Designer wird abgeschafft.

- Die Visual Studio Code-Erweiterung für die HTML-Anwendungsentwicklung wird abgeschafft.
- Die Verwaltung verschiedener Versionen eines kompilierten Projektes mithilfe von Kompilierungszweigen wird abgeschafft.

Systemanforderungen

Stellen Sie vor der Installation von One Identity Manager sicher, dass Ihr System den nachfolgenden minimalen Hardware- und Systemanforderungen genügt. Für detaillierte Informationen zu den Systemvoraussetzungen lesen Sie das *One Identity Manager Installationshandbuch*.

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

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

Minimalanforderungen für Datenbankserver

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

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

Betriebssystem	Windows Betriebssysteme • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. UNIX und Linux Betriebssysteme • Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.
Software	Unterstützt werden die Versionen: • SQL Server 2017 Standard Edition (64-Bit) mit aktuellem kumulativen Update • SQL Server 2019 Standard Edition (64-Bit) mit aktuellem kumulativen Update HINWEIS: Das kumulative Update 2 für SQL Server 2019 wird nicht unterstützt. HINWEIS: Aus Performancegründen wird für produktive Systeme der Einsatz der SQL Server Enterprise Edition empfohlen. • Kompatibilitätsgrad für Datenbanken: SQL Server 2017 (140) • Standard-Sortierschema: Case-Insensitiv, SQL_Latin1_General_CP1_CI_AS (Empfehlung) • SQL Server Management Studio (empfohlen)

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

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

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

Minimalanforderungen für Clients

Auf den Clients sind die folgenden Systemvoraussetzungen zu gewährleisten.

Prozessor	4 physische Kerne mit 2 GHz+ Taktung
Arbeitsspeicher	4 GB+ RAM
Freier Festplattenspeicher	1 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows 11 (x64) • Windows 10 (32-Bit oder 64-Bit) mindestens Version 1511 • Windows 8.1 (32-Bit oder 64-Bit) mit dem aktuellen Service Pack
Zusätzliche Software	• Microsoft .NET Framework Version 4.7.2 oder höher • Microsoft Edge WebView2
Unterstützte Browserversionen	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimalanforderungen für Jobserver

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

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

	• Windows Server 2012 R2 • Windows Server 2012 Linux Betriebssysteme • Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden.
Zusätzliche Software	Windows Betriebssysteme • Microsoft .NET Framework Version 4.7.2 oder höher HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers. Linux Betriebssysteme • Mono 5.14 oder höher

Minimalanforderungen für Webserver

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

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

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

Minimalanforderungen für Anwendungsserver

Zur Installation des Anwendungsservers sind die folgenden Systemvoraussetzungen zu gewährleisten.

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

Zusätzliche Software	Windows Betriebssysteme
	• Microsoft .NET Framework Version 4.7.2 oder höher
	• Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.7.2 und den Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions
	  • Web Server > Application Development > ISAPI Filters
	  • Web Server > Security > Basic Authentication
	  • Web Server > Security > Windows Authentication
	  • Web Server > Performance > Static Content Compression

- Web Server > Performance > Dynamic Content Compression

Linux Betriebssysteme

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

Unterstützte Datensysteme

Diese Sektion führt die Datensysteme auf, die durch die Konnektoren dieser One Identity Manager Version unterstützt werden.

Tabelle 43: 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 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.

Konnektor	Unterstützte Datensysteme
	HINWEIS: Es kann der Web Service Assistent, benutzt werden, um die Konfiguration für das Schreiben der Daten zum Web Service zu generieren. Für das Lesen und Synchronisieren der Daten sind zusätzliche Skripte erforderlich, welche die Methoden des Web Service Konnektors nutzen.
Active Directory Konnektor	Active Directory, welches mit Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 und Windows Server 2022 ausgeliefert wird.
Microsoft Exchange Konnektor	• Microsoft Exchange 2010 ab Service Pack 3 • Microsoft Exchange 2013 mit kumulativem Update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 mit kumulativem Update 1 • MicrosoftExchange Hybrid-Umgebungen
SharePoint Konnektor	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019
SAP R/3 Konnektor	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.54 und 7.69 • SAP ECC 5.0 und 6.0 • SAP S/4HANA On-Premise-Edition (auch 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 Safeguard Authentication Services.
Domino Konnektor	• IBM Domino Server Version 8, 9 und 10 • HCL Domino Server Version 11 und 12 • IBM Notes Client 8.5.3 und 10.0 • HCL Notes Client Version 11.0.1 und 12.0 Die 64-Bit-Variante des Notes Client 12.0.1 wird derzeit nicht unterstützt.
Generischer Datenbankkonnektor	• SQL Server • Oracle Database • SQLite

Konnektor	Unterstützte Datensysteme
	• 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 und 7.5
Azure Active Directory Konnektor	• Microsoft Azure Active Directory HINWEIS: Die Synchronisation von Azure Active Directory Mandanten in nationalen Cloud-bereitstellungen mit dem Azure Active Directory Konnektor wird nicht unterstützt. Dies betrifft: • Microsoft Cloud for US Government (L5) • Microsoft Cloud Germany • Azure Active Directory und Microsoft 365 betrieben von 21Vianet in China Weitere Informationen finden Sie auch unter https://-support.oneidentity.com/KB/312379. • Microsoft Teams
SCIM Konnektor	Unterstützt werden Cloud-Anwendungen, welche die System for Cross-domain Identity Management (SCIM) Spezifikation in der Version 2.0 verstehen. Die Anforderungen von RFC 7643 (System for Cross-domain Identity Management: Core Schema) und RFC 7644 (System for Cross-domain Identity Management: Protocol) sind zu gewährleisten.
Exchange Online Konnektor	• Microsoft Exchange Online
Google Workspace Konnektor	• Google Workspace

Konnektor	Unterstützte Datensysteme
Oracle E-Business Suite Konnektor	• Oracle E-Business Suite System Version 12.1 und 12.2
SharePoint Online Konnektor	• Microsoft SharePoint Online
One Identity Safeguard Konnektor	• One Identity Safeguard Version 6.0, 6.7, 6.10 und 6.11

Produktlizenzierung

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

Upgrade und Installationsanweisungen

Um One Identity Manager 8.2.1 erstmals zu installieren, folgen Sie den Installationsanweisungen im *One Identity Manager Installationshandbuch*. Ausführliche Anweisungen für die Aktualisierung finden Sie im *One Identity Manager Installationshandbuch*.

> WICHTIG: Beachten Sie die Hinweise zur Aktualisierung des One Identity Manager auf Seite 58.

Hinweise zur Aktualisierung des One Identity Manager

- Bevor Sie ein Migrationspaket in ein Produktivsystem einspielen, testen Sie die Änderungen zunächst in einer Testumgebung. Verwenden Sie eine Kopie der produktiven Datenbank für die Tests.
- Stellen Sie vor der Aktualisierung der One Identity Manager-Datenbank auf die Version 8.2.1 sicher, dass der administrative Systembenutzer, mit dem die Kompilierung der Datenbank erfolgt, ein Kennwort hat. Anderenfalls kann die Aktualisierung des Schemas nicht vollständig durchgeführt werden.
- Für eine One Identity Manager-Datenbank auf einem SQL Server wird aus Performancegründen empfohlen, für die Zeit der Schemaaktualisierung die

Datenbank auf das Wiederherstellungsmodell **Einfach** zu setzen.

- Während der Aktualisierung einer One Identity Manager-Datenbank der Version 8.0.x auf die Version 8.2.1 werden diverse Spalten zu physischen Pflichtfeldern, die bereits semantisch als Pflichtfelder definiert waren.

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

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

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

  UPDATE fails
  ```

  Prüfen und korrigieren Sie vor der Aktualisierung einer One Identity Manager-Datenbank die Daten. Im Add-on für das Konfigurationsmodul auf dem Installationsmedium wird ein Prüfskript bereitgestellt (`\SDK\SQLSamples\MSSQL2K\30374.sql`). Im Fehlerfall korrigieren Sie die Daten und starten Sie die Aktualisierung erneut.

- One Identity Manager nutzt In-Memory-OLTP (Online Transactional Processing - Onlinetransaktionsverarbeitung) für speicheroptimierte Datenzugriffe.
  Der Datenbankserver muss die extreme Transaktionsverarbeitung (XTP) unterstützen. Ist XTP nicht aktiviert, wird die Installation oder Aktualisierung nicht gestartet. Prüfen Sie, ob für den SQL Server die Eigenschaft **Extreme Transaktionsverarbeitung unterstützt** (Is XTPSupported) auf den Wert **True** gesetzt ist.

  Für die Erstellung speicheroptimierter Tabellen sind folgende Voraussetzungen zu erfüllen:

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

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

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

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

  Stellen Sie daher vor der Aktualisierung der Datenbank sicher, dass Sie ein entsprechendes Verfahren zur Datenarchivierung konfiguriert haben. Ausführliche

Informationen zur Archivierung von Daten finden Sie im *One Identity Manager Administrationshandbuch für die Datenarchivierung*.

- Für den Zeitraum der Aktualisierung wird die Datenbank in den Einzelbenutzermodus gesetzt. Beenden Sie alle bestehenden Verbindungen zur Datenbank vor dem Start der Schemaaktualisierung.
- Bei Einsatz einer Datenbankspiegelung kann es zu Problemen bei der Aktivierung des Einzelbenutzermodus kommen.
- Während der Installation einer neuen One Identity Manager-Datenbank oder einer neuen One Identity Manager History Database mit der Version 8.2.1 sowie der Aktualisierung einer One Identity Manager-Datenbank oder One Identity Manager History Database von Version 8.0.x auf die Version 8.2.1 können Sie festlegen, ob Sie mit abgestuften Berechtigungen auf Serverebene und Datenbankebene arbeiten möchten. Dabei werden durch den Configuration Wizard SQL Server Anmeldungen und Datenbankbenutzer mit den erforderlichen Berechtigungen für den administrative Benutzer, Konfigurationsbenutzer und Endbenutzer erstellt. Ausführliche Informationen zu den Berechtigungen finden Sie im *One Identity Manager Installationshandbuch*.

  Passen Sie nach der Aktualisierung des One Identity Manager die Verbindungsparameter an. Die betrifft beispielsweise die Verbindungsinformationen für die Datenbank (`DialogDatabase`), den One Identity Manager Service, die Anwendungsserver, die Administrations- und Konfigurationswerkzeuge, die Webanwendungen und die Webservices sowie die Verbindungsinformationen in Synchronisationsprojekten.

  > HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 8.2.1 auf das abgestufte Berechtigungskonzept wechseln möchten, verwenden Sie einen Installationsbenutzer mit den Berechtigungen für dieses Rechtekonzept. Ausführliche Informationen zu den Berechtigungen finden Sie im *One Identity Manager Installationshandbuch*.
  >
  > Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

- Damit die Kompilierung von HTML-Anwendungen mit dem Configuration Wizard erfolgreich durchgeführt werden kann, müssen Pakete aus dem NPM-Repository heruntergeladen werden. Stellen Sie daher sicher, dass die Arbeitsstation, auf der der Configuration Wizard ausgeführt wird, eine Verbindung zur Webseite https://registry.npmjs.org herstellen kann.

  Alternativ ist es möglich, die Pakete von einem Proxy-Server herunterzuladen und manuell zur Verfügung zu stellen. Weitere Informationen finden Sie im Knowledge Artikel unter https://support.oneidentity.com/kb/266000.
- Nach Beenden der Aktualisierung wird die Datenbank automatisch in den Mehrbenutzermodus geschaltet. Sollte dies nicht möglich sein, erhalten Sie eine Meldung, über die Sie die Datenbank manuell in den Mehrbenutzermodus schalten können.
- Mit der Installation dieser Version benötigen Benutzer, die auf die REST API im Anwendungsserver zugreifen sollen, die Programmfunktion **Erlaubt den Zugriff**

auf die REST API des Anwendungsservers (`AppServer_API`). Weisen Sie den Benutzern diese Programmfunktion zu. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Aktualisieren des One Identity Manager auf Version 8.2.1

WICHTIG: Beachten Sie die Hinweise zur Aktualisierung des One Identity Manager auf Seite 58.

Um eine bestehende One Identity Manager Installation auf die Version 8.2.1 zu aktualisieren

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

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

      HINWEIS:
      - Um eine One Identity Manager Active Directory Edition zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager Active Directory Edition**.
      - Um eine One Identity Manager History Database zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.
   c. Klicken Sie **Installieren**.

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

      WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation.

Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.

3. Beenden Sie den One Identity Manager Service auf dem Aktualisierungsserver.
4. Erstellen Sie eine Sicherung der One Identity Manager-Datenbank.
5. Prüfen Sie, ob der Kompatibilitätsgrad der Datenbank auf den Wert **140** eingestellt ist und passen Sie die Wert bei Bedarf an.
6. Führen Sie die Schemaaktualisierung der One Identity Manager-Datenbank aus.
   - Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation und folgen Sie den Anweisungen.

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

     HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 8.2.1 auf das abgestufte Berechtigungskonzept wechseln möchten, verwenden Sie einen Installationsbenutzer mit den Berechtigungen für dieses Rechtekonzept. Ausführliche Informationen zu den Berechtigungen finden Sie im *One Identity Manager Installationshandbuch*.

     Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.
7. Aktualisieren Sie den One Identity Manager Service auf dem Aktualisierungsserver.
   a. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
   b. Wechseln Sie auf den Tabreiter **Installation**. Wählen Sie die Edition, die Sie installiert haben.
      - Um eine One Identity Manager Active Directory Edition zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity ManagerActive Directory Edition**.
      - Um eine One Identity Manager History Database zu aktualisieren, wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.
   c. Klicken Sie **Installieren**.

      Der Installationsassistent wird gestartet.

d. Folgen Sie den Installationsanweisungen.

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

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

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

Um Synchronisationsprojekte auf die Version 8.2.1 zu aktualisieren

1. Wenn Sie Synchronisationsprojekte für die Anbindung von Cloud-Anwendungen im Universal Cloud Interface eingerichtet haben, aktualisieren Sie in diesen Synchronisationsprojekten das Zielsystemschema. Verwenden Sie den Synchronization Editor.
2. Beim Aktualisieren des One Identity Manager werden gegebenenfalls Änderungen an den Systemkonnektoren oder der Synchronization Engine bereitgestellt. Damit alle bereits eingerichteten Zielsystemsynchronisationen weiterhin fehlerfrei ausgeführt werden, müssen diese Änderungen auf bestehende Synchronisationsprojekte angewendet werden. Dafür werden Patches bereitgestellt.

   HINWEIS: Einige Patches werden automatisch angewendet. Dafür wird ein Prozess in die Jobqueue eingestellt, der alle vorhandenen Synchronisationsprojekte migriert. Damit der Prozess ausgeführt werden kann, muss der One Identity Manager Service auf dem Datenbankserver und auf allen Synchronisationsservern gestartet sein.

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

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

   Weitere Informationen finden Sie unter Anwenden von Patches für Synchronisationsprojekte auf Seite 65.

Um einen Anwendungsserver auf die Version 8.2.1 zu aktualisieren

- Nach der Schemaaktualisierung der One Identity Manager-Datenbank startet der Anwendungsserver die automatische Aktualisierung.
- Um die Aktualisierung manuell zu starten, öffnen Sie die Statusseite des Anwendungsservers im Browser und verwenden Sie den Eintrag **Update immediately** im Menü des angemeldeten Benutzers.

Um das Web Designer Web Portal auf die Version 8.2.1 zu aktualisieren

HINWEIS: Bevor Sie das Web Designer Web Portal aktualisieren:

- Stellen Sie sicher, dass der Anwendungsserver aktualisiert ist.
- Stellen Sie sicher, dass Microsoft Edge WebView2 auf dem Webserver installiert ist.

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

Um einen API Server auf die Version 8.2.1 zu aktualisieren

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

Um das Web Portal für Betriebsunterstützung auf die Version 8.2.1 zu aktualisieren

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

Um die Manager Webanwendung auf die Version 8.2.1 zu aktualisieren

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

Anwenden von Patches für Synchronisationsprojekte

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

Bevor Sie einen Patch anwenden

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

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

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

Um Patches anzuwenden

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

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

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

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

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

7. Prüfen Sie anhand des Patchprotokolls, ob kundenspezifische Anpassungen nachbearbeitet werden müssen.
8. Falls erforderlich, überarbeiten Sie die kundenspezifischen Anpassungen in der Synchronisationskonfiguration.
9. Führen Sie eine Konsistenzprüfung durch.
10. Simulieren Sie die Synchronisation.
11. Aktivieren Sie das Synchronisationsprojekt.
12. Speichern Sie die Änderungen.

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

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

Siehe auch:

- Änderungen an Synchronisationsvorlagen auf Seite 30
- Patches für Synchronisationsprojekte auf Seite 32

Prüfen der erfolgreichen Installation

Um festzustellen, ob die Version installiert ist

- Starten Sie den Designer oder den Manager und wählen Sie den Menüeintrag **Hilfe > Info**.

  Auf dem Tabreiter **Systeminformationen** erhalten Sie einen Überblick über Ihre Systemkonfiguration.

  Die Versionsnummer 2021.0011.0019.0100 für alle Module und die Anwendungsversion 8.2 v82-157600 weisen darauf hin, dass diese Version installiert ist.

Zusätzliche Ressourcen

Zusätzliche Informationen sind verfügbar unter:

- One Identity Manager Support
- One Identity Manager Online-Dokumentation
- One Identity Manager Community
- One Identity Manager Trainingsportal

Weltweite Verwendung

Dieser Abschnitt enthält Informationen über die Installation und die Verwendung dieses Produkts in anderen als englischen Konfigurationen, wie etwa denen, die von Kunden außerhalb von Nordamerika benötigt werden. Dieser Abschnitt ersetzt jedoch nicht die Informationen zu den unterstützten Plattformen und Konfigurationen, die an anderen Stellen in der Dokumentation beschrieben sind.

Diese Version ist Unicode-fähig und unterstützt jeden Zeichensatz. Sie unterstützt den simultanen Betrieb mit mehrsprachigen Daten. Diese Version unterstützt die Verwendung der Software in den folgenden Regionen: Nordamerika, Westeuropa und Lateinamerika, Mittel- und Osteuropa.

Diese Version ist in folgenden Sprachen lokalisiert: Deutsch

Diese Version hat die folgenden bekannten Fähigkeiten oder Einschränkungen: Andere Sprachen, die für das Web UI bestimmt sind, werden über das Produkt One Identity Manager Language Pack bereitgestellt.

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.