

One Identity Manager 9.2.1

Versionshinweise

16. Mai 2024, 04:27 Uhr

Diese Versionshinweise stellen Informationen über den One Identity Manager Release Version 9.2.1 zur Verfügung. Es werden alle Änderungen seit One Identity Manager Version 9.2 aufgeführt.

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

One Identity Manager 9.2.1 ist ein Minor Release mit neuen Funktionen und verbessertem Verhalten. Siehe [Neue Funktionen](#) auf Seite 2 und [Verbesserungen](#) auf Seite 4.

Wenn Sie eine One Identity Manager Version aktualisieren, die älter als One Identity Manager 9.2 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

Über One Identity Manager 9.2.1

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 dem One Identity Manager können Sie Access-Governance-Anforderungen in Ihrem gesamten Konzern plattformübergreifend verwirklichen. One Identity Manager basiert auf einer prozessoptimierten Architektur und realisiert, im Gegensatz zu "traditionellen" Lösungen, die wesentlichen Identity- und Access-Management-Herausforderungen mit einem Bruchteil an Komplexität, Zeitaufkommen und Kosten.

One Identity Starling

Starten Sie Ihr Abonnement in Ihrem One Identity On-Prem-Produkt und verbinden Sie Ihre On-Prem-Lösungen mit unserer Cloud-Plattform One Identity Starling. Ermöglichen Sie Ihrem Unternehmen den sofortigen Zugriff auf eine Reihe von in der Cloud bereitgestellten Microservices, die die Funktionen Ihrer On-Prem-Lösungen von One Identity erweitern. Wir werden One Identity Starling ständig neue Produkte und Funktionen zur Verfügung stellen.

Eine kostenlose Testversion unserer One Identity Starling-Angebote sowie die neuesten Produktfeatures erhalten Sie unter <https://www.cloud.oneidentity.com/>.

Neue Funktionen

Neue Funktionen in One Identity Manager 9.2.1.

HTML5-Webanwendungen

- Die Möglichkeit, in Hyperviews in den Webanwendungen zu navigieren, kann nun im Administrationsportal deaktiviert werden.
- Im [One Identity GitHub-Repository](#) wird eine Dokumentation der wichtigsten Angular-Komponenten bereitgestellt.

Zielsystemanbindung

- Active Roles Version 8.1.5 wird im bisherigen Umfang unterstützt.
- One Identity Safeguard Versionen 7.4 und 7.5 werden im bisherigen Umfang unterstützt.
- SAP S/4HANA Cloud 2022 und 2023 mit SAP BASIS 7.57 und 7.58 werden unterstützt.

Es wird ein aktualisierter BAPI-Transport SAPTRANSPORT_70.ZIP bereitgestellt.

- HCL Domino Server Version 14 sowie HCL Notes Client Version 12.0.1, in der 64-Bit-Variante, und 14.0 werden unterstützt.

Auf dem Gateway-Server muss nun eine 64-Bit-Version des HCL Notes Client installiert sein, damit eine Domino-Umgebung synchronisiert werden kann.

- Im OneLogin-Konnektor wurde zur Vermeidung von Verbindungsabbrüchen wegen Überschreitung des X-RATE Limits eine Behandlung des HTTP Status 429 (too many requests) sowie ein Wartemechanismus mit zufälligen, exponentiell steigenden Wartezeiten implementiert. Somit werden abgelehnte Anfragen bis zu einer Stunde lang wiederholt.

Identity Management und Access Governance

- Für Identitäten wird ein neuer Mitarbeitertyp **Werkarbeiter** unterstützt. Der Mitarbeitertyp wird im Lizenzbericht für One Identity Manager berücksichtigt.
- Azure Active Directory Administratorrollen können nun automatisch in den IT Shop aufgenommen werden. Die Funktionalität wird über den Konfigurationsparameter **QER | ITShop | AutoPublish | AADDirectoryRole** aktiviert. Für die Entscheidung von Bestellungen wird standardmäßig die Entscheidungsrichtlinie **Entscheidung der Azure Active Directory Bestellungen** genutzt.

HINWEIS: Die neue Entscheidungsrichtlinie **Entscheidung der Azure Active Directory Bestellungen** wurde ebenfalls an die bereits bestehenden Standardregale für **Unwirksame Azure Active Directory Dienstpläne**, **Azure Active Directory Gruppen** und **Azure Active Directory Abonnements** zugewiesen.

- Prüfen Sie, ob kundendefinierte Entscheidungsrichtlinien für diese Produkte noch wirksam sind.
- Zuweisungen, die durch eine Bestellung zustande gekommen sind, können nun ebenfalls bei negativer Attestierung automatisch entfernt werden. Die folgenden neuen Konfigurationsparameter wurden implementiert:
 - QER | Attestation | AutoRemovalScope | OrgHasESet | RemoveRequested
 - QER | Attestation | AutoRemovalScope | DepartmentHasESet | RemoveRequested
 - QER | Attestation | AutoRemovalScope | LocalityHasESet | RemoveRequested
 - QER | Attestation | AutoRemovalScope | ProfitCenterHasESet | RemoveRequested
- Microsoft Teams Teams und Mitgliedschaften in Teams können attestiert werden. Dafür werden Standard-Attestierungsrichtlinien und Standard-Entscheidungsworkflows bereitgestellt. Der automatische Entzug von Mitgliedschaften in Teams nach abgelehnter Attestierung wird unterstützt.
 - Neues Entscheidungsverfahren **OW - Produkteigner eines Microsoft Teams Teams**
- Unternehmensrichtlinien können so konfiguriert werden, dass für jede Richtlinienverletzung eine Attestierung gestartet wird. Dafür wird der Unternehmensrichtlinie eine Attestierungsrichtlinie zugeordnet. Berechtigungen, die

Unternehmensrichtlinien verletzen, können damit automatisch entfernt oder Benutzerkonten deaktiviert werden. Um die Attestierung zu starten, gibt es drei Möglichkeiten:

- Zeitgesteuert durch den Zeitplan, welcher der Attestierungsrichtlinie zugewiesen ist
- Automatisch, sobald eine Richtlinienverletzung ermittelt wurde
- Manuell, über die Aufgabe **Attestierungsvorgänge jetzt erstellen**

Verwandte Themen

- [Verbesserungen](#) auf Seite 4
- [Gelöste Probleme](#) auf Seite 8
- [Schemaänderungen](#) auf Seite 32
- [Patches für Synchronisationsprojekte](#) auf Seite 35

Verbesserungen

Nachfolgend finden Sie eine Liste von Verbesserungen, die in One Identity Manager 9.2.1 implementiert wurden.

Tabelle 1: Allgemein

Verbesserung	Fehler ID
Zusätzliche zulässige Werte für die Spalte <code>DialogParameter.QueryDisplayType</code> für die verbesserte Darstellung von Daten zu Werteabfragen.	430664, 36621
Verbesserte Performance bei der Berechnung von Berechtigungen für One Identity Manager-Benutzer.	431109, 36836
Die Sicherheit des Hilfesystems wurde erhöht.	437475, 37345
Beim Start einzelner Programme über das Launchpad kann nun gewählt werden, ob eine automatische Anmeldung erfolgen soll oder ob neue Verbindungsinformationen zur Anmeldung verwendet werden sollen.	440485
Verbesserte Dokumentation der Eigenschaft Keine direkte Datenbankverbindung für Jobserver.	440489, 37435
Password Manager Secure Password Extension wurde auf Version 5.13.1 aktualisiert.	442044
Verbesserte Performance bei der Erzeugung und Verarbeitung von Prozessen.	443099

Verbesserung	Fehler ID
Verbesserte Dokumentation des Assistenten zur Eingabe von Datenbankabfragen.	445717
Verbesserte Performance bei Abfragen der Jobserver auf die Jobqueue.	445982
Konfigurationsparameter können nun auch dann als verschlüsselt markiert werden, wenn die Datenbank keine Verschlüsselung konfiguriert hat.	446349
Verbesserte Performance im Job Queue Info beim Laden der Informationen aus der Prozesshistorie.	449818, 453348

Tabelle 2: HTML5-Webanwendungen

Verbesserung	Fehler ID
Im Web Portal kann man nun innerhalb eines Hyperviews von einem Objekt zum anderen navigieren.	427806
Im Web Portal kann man nun einen Link auf die Bestellseite setzen, wobei eine bestimmte Servicekategorie oder ein bestimmtes Produkt geöffnet wird. Verwenden Sie dazu den URL-Parameter /#/newrequest/allProducts?serviceCategory=<UID-der-Servicekategorie> beziehungsweise /#/newrequest/allProducts?serviceItem=<UID-der-Leistungsposition>.	427946
Fehlertexte werden nun nicht nur im HTTP-Statusfeld, sondern auch im Payload der Antwort auf eine API-Anfrage ausgegeben. Dies verbessert die Kompatibilität mit HTTP/2.0	432451
Die Performance des API Servers wurde verbessert.	435696
Im Web Portal werden nun auch die Objekttypen von Objekten angezeigt, die an einem Attestierungsvorgang beteiligt sind.	436245
Wenn OAuth nicht korrekt konfiguriert ist, werden nun aussagekräftigere Fehlermeldungen für das API Server-Protokoll generiert.	437362
Im Web Portal bietet nun der Export von Daten mehr Eigenschaften zur Auswahl an.	439740
Die Registrierung von Angular-CDR-Providern wurde verbessert.	440711
Die Dokumentation zu benutzerdefinierten Designs des GitHub-Repositorys der Standard-HTML-Anwendungen wurde verbessert.	440711
Im Web Portal kann man nun Bestellungen verlängern, auf die man eine Schreibberechtigung hat.	443133
Im Administrationsportal kann man nun mithilfe des Konfigurationsschlüssels VI_ITShop_Filter_AccProduct einen Filter festlegen. Dieser Filter bestimmt, welche Leistungspositionen im	445150

Verbesserung	Fehler ID
Web Portal je nach ausgewählten Bestellempfängern angezeigt werden.	
Im Administrationsportal kann man nun mithilfe des Konfigurationsschlüssels VI_ITShop_Filter_AccProductGroup einen Filter festlegen. Dieser Filter bestimmt, welche Servicekategorien im Web Portal je nach ausgewählten Bestellempfängern angezeigt werden.	445150
Verbesserte Dokumentation zum Docker-Container für den API Server.	449613
Die Drittanbieterkomponente Node.js wurde auf die Version 16.20.2 aktualisiert.	454172

Tabelle 3: Web Designer Webanwendungen

Verbesserung	Fehler ID
Im Web Designer Web Portal wurde die Performance beim Kopieren von Positionen im Einkaufswagen verbessert.	446254
Die Performance beim Absenden des Einkaufswagens im Web Designer Web Portal wurde verbessert, wenn der Konfigurationsschlüssel VI_ITShop_CalculateComplianceCheck deaktiviert ist.	449152

Tabelle 4: Zielsystemanbindung

Verbesserung	Fehler ID
Für die Anwendung von Filtern werden unterschiedliche Strategien genutzt.	35406
Die Beschreibung der Variablen für Microsoft Exchange-Synchronisationsprojekte wurde verbessert.	433874, 37274
Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#37274 bereitgestellt.	
Optimierung des SAP R/3-Konnektors für die Synchronisation von SAP-Berechtigungen, falls die Gesamtzahl der SAP-Berechtigungen für die Verarbeitung zu umfangreich ist. Es werden zusätzliche Synchronisationsschritte angeboten, welche die SAP-Berechtigungen partitioniert verarbeiten.	438884, 37380
Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#37380 bereitgestellt.	

Um die Optimierung zu nutzen

1. Wenden Sie im Synchronization Editor den Patch VPR#37380 an.
2. Aktivieren Sie die Synchronisationsschritte **profileHasAuthObjectFieldPart1**, **profileHasAuthObjectFieldPart2**, **profileHasAuthObjectFieldPart3** und

Verbesserung	Fehler ID
<p>profileHasAuthObjectFieldPart4.</p> <p>3. Deaktivieren Sie den Synchronisationsschritt profileHasAuthObjectField.</p> <p>4. Speichern Sie die Änderungen.</p> <p>Bei der folgenden Synchronisation werden alle SAP-Berechtigungen in vier Blöcke aufgeteilt und unabhängig voneinander verarbeitet.</p>	
Wenn in der NLog-Konfiguration der Informationsgrad Trace aktiviert ist, protokolliert der Microsoft Graph-Konnektor, der für die Synchronisation von Azure Active Directory und Microsoft Teams verwendet wird, nun Anfragen an den Graph-Endpunkt. Das Protokoll enthält nur die Anfrage-URI und den Antwort-Code. Um Anfrage und Antwort abzugleichen, wird eine GUID generiert.	441232
Im Manager werden auf den Formularen für Active Directory Benutzerkonten, Kontakte und Gruppen weitere POSIX-Eigenschaften angezeigt.	441991
Der generische Datenbankkonnektor für PostgreSQL-Datenbanken unterstützt die Datentypen Name und OID.	447959
Bei der Synchronisation auftretende Verbindungstimeouts des SAP .Net Connector werden erkannt und die RFC-Verbindung wird transparent neu aufgebaut.	448633

Tabelle 5: Identity Management und Access Governance

Verbesserung	Fehler ID
Die Entscheidungsverfahren OA und TO wurden erweitert, um Entscheider für Zuweisungsbestellungen zu ermitteln.	430621, 36432
Das Entscheidungsverfahren EN wurde erweitert, um Attestierer für Zuweisungen von Systemberechtigungen an hierarchische Rollen zu ermitteln.	
Verbesserte Abbildung von Verantwortlichkeiten von Identitäten.	430714, 36914
An Geschäftsrollen mit der Rollenklasse Teamrolle können nun alle Arten an Unternehmensressourcen per Zuweisungsbestellung zugewiesen werden.	438994, 37377
Funktionsänderungen im Modul Modul SAP R/3 Compliance Add-on (SAC) wurden auf eine stabile Version zurückgerollt.	447665
Wenn bei der Entscheidung per E-Mail eine Entscheidungsmail nicht verarbeitet werden kann, werden die Entscheider nun über die Fehlersituation informiert und die Entscheidungsmail wird entsprechend dem konfigurierten Aufräumverfahren aus dem Postfach entfernt.	430230

Verbesserung

Fehler ID

Wenn der Versand von E-Mail-Benachrichtigungen über Microsoft Exchange oder Exchange Online scheitert, wird dieselbe E-Mail nun über eine SMTP-Verbindung versendet, sofern diese Möglichkeit konfiguriert ist.

Verwandte Themen

- [Schemaänderungen](#) auf Seite 32
- [Patches für Synchronisationsprojekte](#) auf Seite 35

Gelöste Probleme

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

Tabelle 6: Allgemein

Gelöstes Problem	Fehler ID
Fehler in der Prozessverarbeitung nachdem eine Datenbank aus einer Datenbanksicherung wiederhergestellt wurde. Fehlermeldung: Script assembly WebServices_<...> not found in 'DialogScriptAssembly'.	430839, 35340
Im Configuration Wizard werden beim Wiederherstellen einer Datenbank die Berechnungsaufträge für den DBQueue Prozessor nicht verarbeitet.	430950, 36428
Die Updatemigration von den One Identity Manager Versionen 8.1.x oder 8.2.x mit abgestuften Berechtigungen auf die Versionen 9.0, 9.1 oder 9.2 hinterlässt nicht mehr benötigte Berechtigungen für die msdb-Datenbank. HINWEIS: Nutzen Sie das SDK-Skript <code>Modules\QBM\dvd\AddOn\SDK\SQLSamples\MSSQL2K\SDK_Remove_Rights_on_msdb.sql</code> um nicht mehr benötigte Berechtigungen für die msdb-Datenbank zu entfernen.	430965, 36480
Für die Anmeldung in der Manager Webanwendung funktioniert Single-Sign-On nicht, wenn die Webanwendung über einen Anwendungsserver verbunden ist.	431124, 36849
Die Token-Authentifizierung am Anwendungsserver über OAuth2.0/OpenID Connect am Endpunkt <code>/api/script/...</code> funktioniert nicht.	431256, 37025
Im Report Editor werden Abfragen und Parameter von Berichten beim Speichern nicht an Änderungskennzeichen zugewiesen.	432633, 37212
In der Manager Webanwendung kommt es unter Umständen beim	433747,

Gelöstes Problem	Fehler ID
Doppelklicken auf ein Symbol zu einem Fehler.	37242
In der mit Schema Extension erzeugten Definitionsdatei für View-Tabellen mit Fremdschlüsselbeziehungen fehlen die Informationen zu den Fremdschlüsseln.	433801, 37263
Bei der Anmeldung am Launchpad über OAuth tritt ein Fehler auf.	436327, 37289
Soll eine Bildungsregel für mehrere Objekte gleichzeitig ausgeführt werden, kann es zu Fehlern kommen.	436367, 37307
Wenn der Konfigurationsparameter Common ProcessState PropertyLog AllDefaultPropertiesForModel aktiviert ist, werden nun auch Änderungen an Zuweisungen von Kontendefinitionen an Rollen und Organisationen aufgezeichnet.	438090
Schwellwerte von vordefinierten Statistikdefinitionen sind jetzt durch Kunden konfigurierbar.	438821
Bei der Übernahme von Aufzeichnungen der Prozesshistorie in die History Database kann es zu Fehlern kommen. Fehlermeldung: Cannot insert duplicate key in object 'dbo.HistoryJob'.	438926, 37336
Beim Verwerfen einer Sitzung im Anwendungsserver-Client tritt unter Umständen ein Fehler auf. Fehlermeldung: System.ObjectDisposedException: The session is already disposed.	438971, 37367
Die Aktualisierung der Datenbank von One Identity Manager Version 8.2.x auf Version 9.2.x schlägt fehl. WICHTIG: Bevor Sie eine Datenbank mit der One Identity Manager Version 8.2.x auf eine Version 9.2.x aktualisieren, führen Sie das Skript QBM\Database\MSSQL\040Procedures\QBM_GCommon2\QBM_PWriteDialogJournal.sql in einem geeigneten Programm zur Ausführung von SQL-Abfragen aus.	439671, 37341
Im Job Queue Info kann es bei der Auswahl mehrerer Prozesse zu Fehlern kommen.	439761, 37410
Wenn der Name des SQL Servers Sonderzeichen (beispielsweise \, ? oder :) enthält, wird im Database Transporter ein ungültiger Name für die Transportdatei generiert. Sonderzeichen werden nun mit einem Unterstrich (_) ersetzt.	439766
Zeitpläne werden in bestimmten Konstellationen innerhalb einer Minute zweimal gestartet.	440501, 37439

Gelöstes Problem	Fehler ID
Im Job Queue Info treten unter Umständen Fehler auf, wenn Einträge einer History Database angezeigt werden sollen.	440504, 448996
Die Installation des One Identity Manager-Schemas in eine leere Datenbank schlägt fehl, wenn der verwendete Installationsbenutzer nicht Mitglied der Serverrolle dbcreator ist.	440506, 37442
Kompilierungsfehler bei der Aktualisierung der One Identity Manager-Datenbank auf Version 9.2, wenn in der bestehenden Installation der Konfigurationsparameter QER Policy deaktiviert wurde.	440668
Die Berechnung und Auswertung der Wirksamkeit von historischen Zuweisungen in Berichten ist fehlerhaft.	440795
Beim Transport von Änderungskennzeichen, die Löschoperationen auf Schemadaten enthalten, tritt ein Fehler auf. Fehlermeldung: Das Objekt vom Typ Zusätzliche Sichtdefinitionen existiert nicht in der Datenbank oder Sie haben keine Berechtigungen es zu sehen.	441417
Nach dem Reaktivieren von Prozessschritten werden im Systemprotokoll Warnungen aufgezeichnet.	441496
Wenn der Informationsgrad Debug zur Protokollierung verwendet wird, kommt es unter Umständen zu Fehlern beim Starten der Frontends.	441518
Im Job Queue Info sind Filter in der Prozesshistorie fehlerhaft.	441675, 439759
Das Anklicken von Elementen in der Ergebnisliste löst unter Umständen Drag-and-Drop-Ereignisse aus, die zu Folgefehlern führen können.	441687
Der DBQueue Prozessor Auftrag zum Erstellen der Datenbankserverberechtigungen schlägt fehl, wenn der Schemaname einen Backslash (\) enthält.	441824
Wenn in einem Prozess zum Versenden von E-Mail-Benachrichtigungen der Parameter Address keinen Wert enthält, wird kein Fehler gemeldet.	442110
Die Ermittlung der Zeitzone für den Datenbankserver ist fehlerhaft.	442372
Wenn ein fehlgeschlagener Prozessschritt manuell in den Fehlerzweig oder in den Erfolgsweg geschaltet wird, wird die Information im nächsten ausgeführten Prozessschritt protokolliert.	442773
Wenn der oberste Prozessschritt eines Prozesses verschoben wird, wird nicht erkannt, dass eine Kompilierung notwendig ist.	443440
Mangelnde Performance bei der Ausführung des Wartungsauftrags zum Verkleinern der Prozesshistorie.	445873

Gelöstes Problem	Fehler ID
Fehlende Daten bei der Anzeige von einfachen Listenberichten, die den Standardbericht VI_Reporting_DefaultTemplate als Vorlage verwenden.	445921
Im Job Queue Info werden Filter auf die Tabelle JobHistorie, die in einer älteren One Identity Manager-Version erstellt wurden, nicht mehr angezeigt.	446319
Das Löschen von Einträgen aus dem Systemprotokoll führt unter Umständen zu Performanceproblemen oder zur Blockade der Datenbank.	447189
Bei der Ausführung der Konsistenzprüfung SQL-Clause executeable (QER) tritt unter Umständen ein Fehler auf.	448312
Die englische Länderbezeichnung für die Republik Türkei wurde korrigiert (Türkiye).	448328
Für die Übersetzungsschlüssel Pwd_DeniedChars und Pwd_Quality fehlen die Einträge in der Datenbank. Diese werden bei der Beschreibung vom Kennwortvorschriften genutzt.	448584
Mangelnde Performance nach der Aktualisierung einer History Database.	449127
Wenn Change Data Capture (CDC) für die One Identity Manager-Datenbank aktiviert ist, schlägt die Konsistenzprüfung Missing tables in dialogtable (base) fehl.	454318
Sporadischer Fehler bei der Verarbeitung des DBQueue Prozessor-Auftrags QBM-K-XDateSubItemUpdateFU. Fehlermeldung: Transaction count after EXECUTE indicates a mismatching number of BEGIN and COMMIT statements. Previous count = 1, current count = 2.	454751

Tabelle 7: HTML5-Webanwendungen

Gelöstes Problem	Fehler ID
Im Web Portal bricht unter bestimmten Umständen die Suche ab und ein Fehler wird angezeigt.	298020
Im Web Portal kommt es zum Fehler, wenn man einen Bericht für bereits indirekt zugewiesene Identitäten verfügbar macht.	314229
Im Web Portal ist die Liste der Entscheider und Attestierer nicht vollständig.	418493
Im Web Portal für Betriebsunterstützung wird der Systemstatus nicht korrekt angezeigt.	425740
Bei der Attestierung von PAM Benutzerkonten werden im Web Portal im Datum für die letzte Anmeldung und die letzte Verwendung falsche Uhrzeiten angezeigt.	426940

Gelöstes Problem	Fehler ID
Wenn ein Manager die Regelverletzungen seiner Mitarbeiter auswählt, kann es zu sehr langen Abfragezeiten kommen.	430675, 36684
Im Web Portal liefern Suchen, die Sternchen (*) als Platzhalter enthalten, keine korrekten Ergebnisse.	430895, 36032
Im Web Portal kann für eine Active Directory Gruppe keine Leistungsposition erstellt werden.	430940, 36377
Das Berechnen des Berechtigungsverlusts beim Ablehnen von Attestierungsvorgängen dauert zu lange.	431042, 36691
Im Web Portal werden Bestelleigenschaften für Produkte einer Servicekategorie nicht korrekt an Produkte in einer untergeordneten Servicekategorie übergeben.	431218, 36991
Im Web Portal wird nicht korrekt ermittelt, ob die angemeldete Identität für eine andere Identität verantwortlich ist.	431242, 37011
Im Web Portal wird bei der Entscheidung von Attestierungsvorgängen für neue selbstregistrierte Benutzer die Spalte Sponsor nicht angezeigt.	433416
Im Web Portal für Betriebsunterstützung ist der Tabreiter Kennwörter in der Übersicht für Identitäten leer.	433599
Im Web Portal stimmt unter bestimmten Umständen die Anzeige der gewählten Empfänger bei einer neuen Bestellung nicht mit der tatsächlichen Auswahl überein.	433900
Im Kennwortrücksetzungsportal kann man keine Kennwortfragen bearbeiten.	434134
Im Web Portal können bestimmte Berichte nicht erstellt werden.	438184
Der API Server startet unter Linux nicht.	438416
Im Web Portal dauert das Anzeigen von Benutzerkonten (UNSAccount) im Daten-Explorer zu lange.	438910, 37323
Im Web Portal wird die Anzahl der offenen Bestellungen, Attestierungen und Regelverletzungen nicht aktualisiert.	439550, 446476
Im Web Portal ist es möglich, eine Delegation zu erstellen, obwohl das Pflichtfeld Gültig bis nicht ausgefüllt ist.	439722, 37364
Im Web Portal funktionieren die Suche und die Filter für Produktpakete nicht und verursachen weitere Fehler.	439918
Unter bestimmten Umständen kann man sich nicht mithilfe der Kennwortfragen am Kennwortrücksetzungsportal anmelden, da nicht die richtige Funktion zur Ermittlung des aktuellen Benutzers verwendet wird.	440142
Der API Server extrahiert/verarbeitet die HTML5-Webanwendungen	440193

Gelöstes Problem	Fehler ID
manchmal nicht korrekt.	
Im Web Portal werden nicht alle Bestellparameter für Produkte in den Einkaufswagen übernommen.	440206, 37386
Im Web Portal fehlt in der Liste der Attestierer für einen Attestierungslauf die Scroll-Leiste.	440478
Im Web Portal verursacht das Öffnen der Seite Complianceregeln einen Fehler, wenn man vorher eine benutzerdefinierte Ansicht gespeichert hat.	440720
Ruft man eine URL auf, die die Bestellseite des Web Portals mit einer vordefinierten Suchanfrage öffnet, wird weder das Suchfeld korrekt befüllt noch wird die Suche ausgeführt.	440745
Obwohl die Konfigurationsparameter für die Peer-Gruppen-Analyse deaktiviert wurden (QER ITShop PeerGroupAnalysis CheckCrossfunctionalAssignment, QER Attestation PeerGroupAnalysis CheckCrossfunctionalAssignment, QER ITShop PeerGroupAnalysis, QER Attestation PeerGroupAnalysis), werden weiterhin die dazugehörigen Entscheidungsempfehlungen berechnet und den Benutzern des Web Portals angezeigt.	440964
Die Installation des API Servers mit einem kontobasierten Systembenutzer schlägt fehl.	441944
Im Web Portal für Betriebsunterstützung können Prozessschritte, die nicht auf der Wurzelebene liegen, nicht erneut ausgeführt werden.	442934
Unter bestimmten Umständen wird das Web Portal nicht komplett in der korrekten Sprache angezeigt.	443351
Im Web Portal kommt es zum Fehler, wenn man den Einkaufswagen öffnet, in dem sich ein Produkt befindet, dem keine Servicekategorie zugewiesen ist.	444242
Im Web Portal wird ein Produkt in den Einkaufswagen gelegt, obwohl diese Aktion abgebrochen wurde.	444465
Beim Exportieren von Attestierungsvorgängen aus dem Web Portal werden die Namen beteiligter Objekte nicht korrekt angezeigt.	444713
Das Skript zur Wertermittlung wird nicht korrekt ausgeführt. Somit werden keine Initialwerte für Bestelleigenschaften im Web Portal angezeigt.	445163
Einige Konfigurationseinstellungen des API Servers werden nicht korrekt aus den Konfigurationsdateien geladen.	446293
Fehler beim Erstellen einer Attestierungsrichtlinie im Web Portal, wenn ein Attestierungsverfahren zugewiesen wird, das von einem Standard-	446829

Gelöstes Problem	Fehler ID
Attestierungsverfahren kopiert wurde. Fehler: The SQL statement in the field 'Condition' is not correct. (4373909)	
Im Web Portal können beim Bestellen von Produkten nicht mehr als 20 untergeordnete Servicekategorien einer Servicekategorie angezeigt werden.	446996
Im Web Portal wird auf der Bestellseite nach der Änderung des Empfängers die Liste der Produkte nicht neu geladen.	447002
Im Web Portal werden unter bestimmten Umständen nicht alle Einträge in einer Auswahlliste angezeigt.	447039
Die Farbe der Kopfleiste von HTML5-Webanwendungen kann nicht mithilfe eines benutzerdefiniertem Designs vollständig geändert werden.	447474
Die Anmelden -Schaltfläche der Webanwendungen unterscheidet sich kaum vom Hintergrund und ist daher schlecht zu erkennen.	447713
Im Web Portal werden in den Details eines bestellbaren Produkts nicht alle zugehörigen Berechtigungen angezeigt.	448406
Im Web Portal wird im Organigramm von Identitäten keine Scroll-Leiste angezeigt.	448531
Im Web Portal können Produkteigner keine Bestellungen von Mitgliedschaften in ihren verantworteten Systemberechtigungen abbestellen.	449030
Ist die Präprozessorbedingung RISKINDEX deaktiviert, kann die API nicht mehr kompiliert werden.	449036
Im Web Portal ist es unter bestimmten Umständen nicht möglich, das Format von anzuzeigenden Berichten zu ändern.	449616
Im Web Portal kommt es beim Öffnen eines offenen Attestierungsvorgangs zum Fehler.	450403
Im Web Portal werden in der Historie von Identitäten keine Benutzerkonten angezeigt, wenn die Benutzerkonten zwischenzeitlich gelöscht wurden.	452688
Im Web Portal werden beim Bearbeiten einer dynamischen Rolle bestimmte Werte von Bedingungen immer als deaktiviert angezeigt, obwohl sie aktiviert sind.	453346

Tabelle 8: Web Designer Webanwendungen

Gelöstes Problem	Fehler ID
Unter bestimmten Umständen ist die Auswahlliste Ansichtseinstellungen im Web Designer Web Portal doppelt vorhanden.	430862, 35722

Gelöstes Problem	Fehler ID
Im Web Designer werden Variablen im Code nicht mehr erkannt.	430908, 36145
Unter bestimmten Umständen kommt es im Web Designer Web Portal zu einer Endlosschleife beim Anzeigen und Schließen einer Fehlermeldung.	431050, 36706
Im Web Designer Web Portal werden zeitlich identische Zeitzonen mit unterschiedlichen Namen nicht korrekt unterschieden.	431068, 36765
Unter bestimmten Umständen kann man im Web Designer Monitor keine Protokolle anzeigen.	431165, 36910
Im Web Designer ist es möglich an einem Warnung -Knoten die Option Erweiterte Eigenschaften zu wählen.	431199
Wenn man im Web Designer Web Portal im Einkaufswagen mit vielen Bestellpositionen die Funktion Für alle übernehmen verwendet, ist die Performance schlecht.	431217, 36990
Im Web Designer Web Portal können Hyperviews von Systemberechtigungen nicht angezeigt werden.	438977, 37369
Im Web Designer Web Portal wird fälschlicherweise für die Eigenschaft Deaktivieren bis in den Stammdaten einer Identität eine Uhrzeit-Auswahl angezeigt.	440431
Im Web Web Designer Web Portal werden nicht alle Informationen in einem Hyperview angezeigt.	440490
Im Web Designer Web Portal ist das Bearbeiten von Eigenschaften für mehrere Produkte im Einkaufswagen fehlerhaft.	440970
Im Web Designer Web Portal werden Farbeinstellungen nicht korrekt übernommen.	441410
In den Hyperviews des Web Designer Web Portals sind keine weiterführenden Links mehr vorhanden.	442036, 37436
Im Web Designer Web Portal führt das Drücken der Enter -Taste im Filterdialog unter bestimmten Umständen zum Fehler.	442101
Im Web Designer Web Portal werden einige Zeitzonen nicht korrekt erkannt. Dies verursacht einen Fehler.	442109
Im Web Designer können Übersetzungen nicht manuell angepasst werden.	446017
Im Web Designer Web Portal treten beim Gruppieren von Daten Fehler bei der Anzahl der Gruppen sowie bei der Paginierung auf.	446226
Im Web Designer Web Portal werden in der Historie von Identitäten keine Benutzerkonten angezeigt, wenn die Benutzerkonten zwischenzeitlich gelöscht wurden.	454468

Gelöstes Problem	Fehler ID
Unter bestimmten Umständen kommt es im Web Designer Web Portal beim Generieren von Berichten zum Fehler.	4723794, 33299

Tabelle 9: Zielsystemanbindung

Gelöstes Problem	Fehler ID
Beim Entfernen der Kontendefinition für ein Microsoft Exchange Postfach wird unter Umständen das Active Directory Benutzerkonto gelöscht.	430816, 34839
Fehler bei der Provisionierung ausstehender Cloud Benutzerkonten.	430832, 35201
Änderungen der Telefonnummern einer Identität werden nicht an Exchange Online E-Mail Benutzer mit dem Automatisierungsgrad Full managed weitergereicht.	431043, 36693
Mangelnde Performance beim Laden des Überblickformulars für SAP Benutzerkonten.	431183, 36941
Wenn in einem Synchronisationsprojekt für die Anbindung eines Zielsystems über den Windows PowerShell Konnektor in der Konnektordefinition ein Verbindungsparameter gelöscht wird und anschließend das Zielsystemschemata neu geladen wird, dann wird der Verbindungsparameter in der One Identity Manager-Datenbank (DPRSystemConnection.ConnectionParameter) nicht aktualisiert. HINWEIS: Das Problem tritt nach Installation des Service Packs nicht mehr auf. Wenn in der Konnektordefinition vor Installation des Service Packs ein Verbindungsparameter gelöscht wurde, wenden Sie sich an den Support, um DPRSystemConnection.ConnectionParameter zu bereinigen.	433714, 37223
Der Domino-Konnektor erkennt keine Benutzer und Personendokumente, die kurz vor einer Synchronisation in die One Identity Manager-Datenbank in der Domino-Umgebung neu angelegt wurden.	433740, 37238
Der SCIM-Konnektor kann beim Testen der Verbindungseinstellungen im Projektassistenten keine Verbindung zur Cloud-Anwendung herstellen, wenn OAuth-Authentifizierung genutzt wird und der Verbindungsparameter Sonderzeichen enthält.	433792, 37260
Der Schreibschutz für ein Synchronisationsprojekt, das von mehreren Benutzern gleichzeitig im Synchronization Editor geöffnet ist, funktioniert nicht korrekt.	433795, 37261
Fehler bei der Synchronisation einer SharePoint Online-Umgebung. Fehlermeldung: Duplicate key (reference resolution) Es wird ein Patch für Synchronisationsprojekte mit der Patch ID VPR#37272 bereitgestellt.	433821, 37272
Bei der Auswertung der Simulation einer Synchronisation kann es	436301,

Gelöstes Problem	Fehler ID
sporadisch zu einem Fehler kommen. Fehlermeldung: Object not set to a reference of an object.	37279
Für Identitäten ohne eingetragenen letzten Arbeitstag, sind Benutzerkonten, die über Kontendefinitionen automatisch erzeugt werden, nicht aktiv, da deren Kontoverfallsdatum auf einen Wert in der Vergangenheit gesetzt wird.	436313, 37284
Mitgliedschaften in Azure Active Directory Administratorrollen können nicht gelesen werden.	436354, 37303
Mitgliedschaften in Anwendungsrollen werden bei der Synchronisation mit dem CSV-Konnektor nicht geschrieben, wenn als Schlüssel-eigenschaft im Mapping der Primärschlüssel der Tabelle Person verwendet wird.	436363, 37306
Beim Laden von LDAP Gruppen mit vielen Mitgliedern tritt ein Fehler auf. Fehlermeldung: Invalid data. Data of type (System.Object[]) is not supported.	438967, 37365
Fehler beim Lesen des Schemas einer PostgreSQL-Datenbank. Fehlermeldung: [System.OverflowException] Die arithmetische Operation hat einen Überlauf verursacht.	438984, 37371
Nach Änderung der Mitgliedschaft in einer Systemberechtigung wird der DBQueue Prozessor-Auftrag zur Aktualisierung der Spalte XDateSubItem nicht zurückgestellt, obwohl Verarbeitungsaufträge für das selbe Objekt in der Jobqueue vorhanden sind.	438992, 37376
Gruppenmitgliedschaften von Azure Active Directory Benutzerkonten werden gelöscht, wenn die entsprechenden Mitgliedschaften in Exchange Online aktiv werden.	439006, 37384
Bei der Synchronisation von SAP Berechtigungsobjekten werden nicht alle Objekte der Tabelle USOBHASH in die One Identity Manager-Datenbank eingelesen, wenn in der synchronisierten SAP R/3-Umgebung die SAP BASIS Version 7.57 (SAP S/4HANA 2022) oder neuer eingesetzt wird. Spielen Sie den aktuellen Transport SAPTRANSPORT_70.ZIP in das zu synchronisierende SAP R/3-System ein. Dieser verwendet den Funktionsbaustein /VIAENET/LISTUSOBHASH anstelle des SAP-Bausteins AUTH_TRACE_GET_USOBHASH. Beim Zugriff auf eine SAP R/3-Umgebung prüft der SAP R/3-Konnektor, ob der Funktionsbaustein /VIAENET/LISTUSOBHASH vorhanden ist und verwendet diesen. Damit werden alle Objekte der Tabelle USOBHASH synchronisiert. Im Synchronisationsprotokoll wird aufgezeichnet, ob der Funktionsbaustein /VIAENET/LISTUSOBHASH verwendet wird.	440164
Fehler beim Herstellen einer Remoteverbindung im Synchronization Editor.	440477, 37430

Gelöstes Problem	Fehler ID
Fehlermeldung: An existing connection was forcibly closed by the remote host.	
Einige Spalten für PAM Assetgruppen und PAM Kontogruppen sind zu kurz.	440493, 37437
Fehler beim Schreiben von Daten in Tabellen einer PostgreSQL-Datenbank, wenn die Tabelle eine Spalte enthält, deren Wert automatisch inkrementiert wird.	440899
Bei der Exchange Online Synchronisation tritt unter Umständen ein Fehler auf. Fehlermeldung: You must call Connect-ExchangeOnline before calling any other cmdlet.	440909
Wenn das Token-Verzeichnis für die Azure Active Directory-Deltasynchronisation nicht richtig konfiguriert ist, wird ein aussagekräftigerer Fehler ausgegeben.	441249
Systembenutzer, welche nur Leseberechtigungen haben, konnten im Formular für Objekte des Zielsystemabgleichs trotzdem Objekte löschen, zurücksetzen und publizieren.	441968
Beim Laden von LDAP-Synchronisationsprojekten aus älteren One Identity Manager-Versionen tritt ein Fehler auf.	442114
Fehler beim Einrichten der Synchronisation mit dem generischen Datenbankkonnektor für den generischen ADO.NET-Provider, SAP HANA-Datenbanken und DB2 (LUW)-Datenbanken, wenn die Verbindungskonfiguration aus einer UDL-Datei geladen wird. Fehlermeldung: DistributionConnector: Error connecting the system. Unable to load the UDL file.	442883
Wenn in einer Startfolge mehrere Synchronisationen parallel ausgeführt werden und mindestens zwei Synchronisationen gleichzeitig beendet werden, kann es vorkommen, dass die Startfolge nicht zu Ende ausgeführt wird.	443582
Fehler beim Herstellen der Verbindung zu einer Cloud-Anwendung mit dem SCIM-Konnektor bei Authentifizierung über das OAuth-Protokoll 2.0. Es wird ein Patch für Synchronisationsprojekte mit der Patch ID ADO#444262 bereitgestellt.	444262
Im Manager kann beim Anlegen eines neuen Active Directory Kontakts auf dem Stammdatenformular keine Kontendefinition ausgewählt werden.	444696
Fehler beim Erstellen eines Synchronisationsprojektes mit dem One Identity Manager-Konnektor, wenn die verbundene Datenbank älter als Version 9.0 ist.	444875

Gelöstes Problem	Fehler ID
Fehler im One Identity Manager-Konnektor beim Verbinden mit einer Datenbank der Version 8.2. Fehler: Invalid column name 'SyncInfo'.	445135
Zuweisungen von Cloud Benutzerkonten zu Cloud Gruppen werden bei der Synchronisation unter folgenden Voraussetzungen nicht in der One Identity Manager-Datenbank gelöscht: <ul style="list-style-type: none"> • Die Synchronisation ist so konfiguriert, dass Objekte, die nur in der Datenbank vorhanden sind, sofort gelöscht werden. • Es handelt sich um direkte Zuweisungen. • Für die Tabelle CSMUserInGroup ist Zuweisung per Ereignis aktiviert. 	445879
Für Zielsystemobjekte, die über eine Remoteverbindung in die One Identity Manager-Datenbank eingelesen werden, kann mitunter der Anzeigename nicht korrekt gebildet werden.	446392
Im Bericht über die Simulation einer Synchronisation mit Revisionsfilterung fehlen einzelne Schritte.	446827
One Identity Safeguard Benutzer, welche als Identitätsanbieter ein Active Directory verwenden, können nicht aus lokalen One Identity Safeguard Benutzergruppen entfernt werden.	447214
Die Spalte O3EMailbox.AdditionalResponse ist zu kurz.	447424
Bei der Reaktivierung eines fehlgeschlagenen Prozesses zur Anlage von Active Directory Benutzerkonten kann es im Einzelfall dazu kommen, dass ein Benutzerkonto trotz ursprünglich gesetztem Kennwort ohne Kennwort angelegt wird.	448865
Mangelnde Performance beim Laden der Azure Active Directory Rollenberechtigungen.	449166
Die Exchange Online Postfachberechtigungen für den Vollzugriff werden nicht korrekt synchronisiert.	449217
Fehler bei der Simulation einer Synchronisation, wenn für die Verbindung zum Zielsystem eine Remoteverbindung genutzt wird.	450049
Beim Einrichten der Systemverbindung zu einer Oracle Database mit dem generischen Datenbankkonnektor werden Spalten als eindeutiger Schlüssel ausgewählt, die NULL -Werte zulassen.	450660
Bei der Konfiguration einer Synchronisation mit dem generischen Datenbankkonnektor können Spalten mit dem Datentyp Integer nicht als bevorzugter Schlüssel ausgewählt werden.	450662
Die virtuelle Eigenschaft zur Datenkonvertierung verursacht einen Fehler	452616

Gelöstes Problem	Fehler ID
bei der Konvertierung von Datumsangaben, wenn die Zeitzone des Basiswertes von der lokalen Zeitzone abweicht.	
Objekte, die keine Änderungen, aber nicht auflösbare Mitgliedschaften enthalten, belasten die Quota, die im Synchronisationsschritt festgelegt ist. Das kann zum Abbruch der Synchronisation führen.	452674
Ausstehende Azure Active Directory-Objekte werden im Manager nicht im Zielsystemabgleich angezeigt.	453248
Nach der Umstellung auf die Version 3.1 des SAP .Net Connector wurden ab Patch 3 mitunter Zuweisungen von SAP Rollen zu SAP Benutzerkonten nicht synchronisiert, weil das zugehörige Benutzerkonto nicht gefunden wurde.	454283

Tabelle 10: Identity Management und Access Governance

Gelöstes Problem	Fehler ID
Mangelnde Performance beim Laden der Liste von Attestierungsvorgängen.	431058, 438951, 444125, 36739
Zu umfangreiche Berechtigungen eines Managers zum Anlegen neuer Abteilungen, Standorte, Kostenstellen oder Geschäftsrollen.	431370, 37129
Bei der Delegation von Verantwortlichkeiten für hierarchische Rollen wird im Bestellvorgang der Wert für Rolle/Organisation (PersonWantsOrg.ObjectKeyOrgUsedInAssign) nicht korrekt gebildet.	431390, 37142
Ein Delegierender erhält irrelevante Benachrichtigungen über die Entscheidung von Bestellungen.	433752, 37243
Mangelnde Performance beim Löschen eines IT Shop Regals.	436343, 37296
Wenn eine Identität eine Bestellung gleichzeitig als regulärer Entscheider und als Mitglied der zentralen Entscheidergruppe entscheiden kann, wird in der Entscheidungshistorie mitunter nicht der reguläre Entscheider, sondern die zentrale Entscheidergruppe als Entscheider aufgezeichnet.	436371, 37308
Unter bestimmten Bedingungen werden E-Mail-Benachrichtigungen über die Genehmigung einer Bestellung nicht versendet, obwohl E-Mail-Benachrichtigungen korrekt konfiguriert sind.	438917, 37328
Wenn ein Produkt abbestellt wird, während der Prozess zur Verlängerung der Bestellung läuft, dann wird der Verlängerungsworkflow anstelle des Abbestellworkflows ausgeführt.	438935, 37344
Für die Entscheidungsverfahren XM, CM und PW werden die Attestierer nicht neu berechnet, wenn ein Attestierer die Entscheidung delegiert hat.	438946, 37354

Gelöstes Problem	Fehler ID
In einem mehrstufigen Genehmigungsverfahren mit automatischen Entscheidungen, wird eine Bestellung abgelehnt, obwohl der Konfigurationsparameter DecisionOnInsert aktiviert ist. Der Fehler tritt auf, wenn nach einer negativ entschiedenen Entscheidungsebene der Besteller in weiteren Ebenen auch entscheidungsberechtigt ist.	438980, 37370
Für Produkteigner werden zu einer Leistungsposition zu wenige Informationen angezeigt.	439011, 37387
Die Funktion SAC_FTPProfileInSAPFunction liefert falsche Ergebnisse, wenn eine SAP Funktion aus mehr als einer Transaktion besteht. Das führt zu unerwarteten Ergebnissen, abhängig von der Reihenfolge der Transaktionen innerhalb der SAP Funktion.	439016, 37389
Fehlerhafte Neuberechnung der Attestierer, wenn ein regulärer Attestierer initial auch Mitglied der zentralen Entscheidergruppe ist und später aus dieser Gruppe entfernt wird.	439757, 37407
Der Customizer verhindert die Zuweisung von Azure Active Directory Gruppen, unwirksamen Azure Active Directory Dienstplänen und Azure Active Directory Abonnements zum IT Shop.	440848
Mitunter werden IT Shop-Bestellungen abgebrochen, wenn ein Regal in einen anderen Shop verschoben wird, obwohl an der Leistungsposition Bestellung bleibt bei Umzug bestehen aktiviert ist.	441274
Wenn ein Entscheidungsschritt eskaliert wird, wird die Bestellung unter folgenden Bedingungen automatisch abgebrochen und nicht den Eskalationsentscheidern vorgelegt: <ul style="list-style-type: none"> • Ein Entscheider aus dem folgenden Entscheidungsschritt zur Eskalation eskaliert die Bestellung manuell. • Der Konfigurationsparameter QER ITShop AutoDecision ist aktiviert. 	441330
Die Produkteigner von Systemrollen, abonnierbaren Berichten und Software können die Überblicksformulare des verantworteten Produktes nicht sehen.	442050
Fehler beim Bestellen einer Cloud Gruppe, wenn dieser Gruppe ein Cloud Berechtigungselement zugewiesen ist.	442501
Gelegentliche Performanceprobleme bei der Verarbeitung des DBQueue Prozessor-Auftrags QER-K-PWOHelperFillMakeProc.	443432
Auf dem Stammdatenformular für Richtlinienverletzungen funktionieren die Links zu Objekt und Richtlinie nicht mehr.	443827
An verschiedenen Zuweisungstabellen fehlt die Methode CreateITShopOrder.	452721

Gelöstes Problem	Fehler ID
Mangelnde Performance beim Zuweisen von Identitäten zu Anwendungsrollen.	453161
Fehler bei der Ausführung des Prozesses VI_Attestation_AttestationHelper send mail new task for approver auf einem Jobserver, der über einen Anwendungsserver verbunden ist.	453288

Verwandte Themen

- [Schemaänderungen](#) auf Seite 32
- [Patches für Synchronisationsprojekte](#) auf Seite 35

Bekannte Probleme

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

Tabelle 11: Allgemein

Bekanntes Problem	Fehler ID
Fehler im Report Editor, wenn im Bericht Spalten verwendet werden, die im Report Editor als Schlüsselworte definiert sind. Workaround: Erstellen Sie Datenabfragen als SQL-Abfragen und nutzen Sie für die betroffenen Spalten Aliasnamen.	23521
Wird der Web Installer gleichzeitig in mehreren Instanzen gestartet, kann es zu Zugriffsfehlern kommen.	24198
Header-Zeilen in als CSV gespeicherten Reporten enthalten keine sprechenden Namen.	24657
Im Configuration Wizard können unzulässige Modulkombinationen ausgewählt werden. Dies führt erst bei Beginn der Schemainstallation zu Fehlern. Ursache: Der Configuration Wizard wurde direkt gestartet. Lösung: Verwenden Sie zur Installation der One Identity Manager Komponenten immer die autorun.exe. Damit ist sichergestellt, dass keine unzulässigen Modulkombinationen ausgewählt werden.	25315
Fehler bei der Verbindung über einen Anwendungsserver, wenn der private Schlüssel des Zertifikates, mit dem die VI.DB ihre Session-Information zu verschlüsseln versucht, nicht exportiert werden kann und der private Schlüssel damit der VI.DB nicht zur Verfügung steht.	27793

Bekanntes Problem	Fehler ID
<p>Lösung: Markieren Sie den privaten Schlüssel beim Export und Import des Zertifikats als exportierbar.</p>	
<p>Fehler beim Auslösen von Ereignissen auf eine View , welche keine UID-Spalte als Primärschlüssel besitzt.</p> <p>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.</p> <p>Die Definition einer View, die als Primärschlüssel den xObjectKey verwendet, ist nicht zulässig und wird an sehr vielen Stellen zu weiteren Fehlern führen.</p> <p>Zur Überprüfung des Schemas wird eine Konsistenzprüfung Table of type U or R with wrong PK definition bereitgestellt.</p>	29535
<p>Wenn die One Identity Manager-Datenbank in einem SQL-Cluster (High Availability 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.</p> <p>Lösung: Deaktivieren Sie die Option DTC_SUPPORT = PER_DB.</p>	30972
<p>Ist explizit kein Datum angegeben, wird intern das Datum 30.12.1899 verwendet. Dies ist bei Wertevergleichen zu beachten, beispielsweise bei der Verwendung in Berichten. Ausführliche Informationen zur Verwendung von Datumsangaben in Berichten finden Sie im <i>One Identity Manager Konfigurationshandbuch</i>.</p>	31322
<p>In einem Bericht werden Variablen verwendet und für diese Variablen sind im Report Editor kundenspezifische Übersetzungen erfasst. Im generierten Bericht werden die Variablen jedoch nicht übersetzt.</p> <p>Ursache: Übersetzungen von Standardvariablen, die im Wörterbuch des Reportdesigners unterhalb der Kategorie Quest angezeigt werden, werden beim Generieren von Berichten mit den Werten aus der One Identity Manager-Datenbank überschrieben.</p> <p>Lösung: Legen Sie eigene Variablen an, die im Wörterbuch des Reportdesigners außerhalb der Kategorie Quest angeordnet sind. Diese Variablen können übersetzt werden.</p>	36686
<p>Die Konsistenzprüfung Columns of type varchar(38) not PK and not FK. erkennt Verstöße für Spalten mit einer Länge von varchar(38), die nicht als UID-Spalten gekennzeichnet sind.</p> <p>Lösung: Wählen Sie bei der Schemerweiterung eine andere Spaltenlänge. Entsprechend der Modellierungsrichtlinien sind Spalten mit einer Länge von varchar(38) reserviert für Spalten, die eine UID abbilden.</p>	37072

Tabelle 12: Webanwendungen

Bekanntes Problem	Fehler ID
<p>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.</p> <p>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.</p>	26739
<p>Die Bestelleigenschaften eines Produktes werden bei der Verlängerung oder Abbestellung im Web Portal nicht aus der ursprünglichen Bestellung in den Warenkorb übernommen.</p> <p>Ursache: Bestelleigenschaften können in unterschiedlichen, kundenspezifischen Spalten gespeichert werden.</p> <p>Lösung: Erstellen Sie eine Bildungsregel für die (kundenspezifische) Spalte an der Tabelle ShoppingCartItem, in der die Bestelleigenschaft bei der Bestellung gespeichert wird. Diese Bildungsregel muss die Bestelleigenschaften für die verknüpfte Bestellung aus der identischen (kundenspezifischen) Spalte an der Tabelle PersonWantsOrg auslesen.</p>	32364
<p>Es ist nicht möglich mithilfe des Web Designer in der Kopfzeile neben dem Firmennamen/-logo einen Link im Web Portal zu platzieren.</p>	32830
<p>Es ist möglich im Web Portal einen Bericht zu abonnieren, ohne dabei einen Zeitplan auszuwählen.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> • Erstellen Sie eine Erweiterung auf das entsprechende Formular, mit der unter der Auswahlliste ein Hinweistext angezeigt wird, der auf das Problem hinweist. • Legen Sie einen Standard-Zeitplan für abonnierbare Berichte fest. • Ändern Sie im Web Designer den Konfigurationsschlüssel Filter für abonnierbare Berichte (VI_Reporting_Subscription_FilterRPSSubscription) und setzen Sie den Wert von Minimale Anzahl Zeichen des Zeitplans (UID_DialogSchedule) auf 1. 	32938
<p>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:</p> <p>System.InvalidOperationException: Method may only be called on a Type for which Type.IsGenericParameter is true.</p> <p>at System.RuntimeType.get_DeclaringMethod()</p>	33867

Bekanntes Problem

Fehler ID

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>
```

Im Web Portal werden in der Detailanzeige eines offenen Attestierungsvorgangs nicht die erwarteten Felder angezeigt, wenn nicht das Standard-Attestierungsverfahren verwendet wird, sondern eine Kopie dessen.

34110

Lösung:

- Die objektabhängigen Verweise des Standard-Attestierungsverfahrens müssen auch für das kundendefinierte Attestierungsverfahren übernommen werden.

Tabelle 13: Zielsystemanbindung

Bekanntes Problem	Fehler ID
Bei PowerShell-Verbindungen, welche intern <code>Import-PSSession</code> 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 <code>EntryDate</code> .	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	27126

Bekanntes Problem	Fehler ID
<p>((Server))).</p> <p>Wahrscheinliche Ursache: Die HCL Domino-Umgebung wurde neu aufgebaut oder es wurden zahlreiche Einträge in das Domino-Verzeichnis eingefügt.</p> <p>Lösung: Aktualisieren Sie in der HCL Domino-Umgebung die Indexe im Domino-Verzeichnis manuell.</p>	
<p>Der SAP-Konnektor stellt keine Schemaeigenschaft bereit, um zu erkennen, ob ein Benutzer in der SAP R/3-Umgebung ein produktives Kennwort hat.</p> <p>Wenn diese Information im One Identity Manager zur Verfügung stehen soll, erweitern Sie das Schema und die Synchronisationskonfiguration.</p> <ul style="list-style-type: none"> • 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
<p>Fehler bei der Provisionierung von Lizenzen in das Tochtersystem einer Zentralen Benutzerverwaltung.</p> <p>Meldung: No company is assigned.</p> <p>Ursache: Für das Benutzerkonto konnte keine Firmenadresse ermittelt werden.</p> <p>Lösung: Stellen Sie sicher, dass entweder</p> <ul style="list-style-type: none"> • jedem Benutzerkonto eine Firma zugeordnet ist, die im Zentralsystem existiert <li style="padding-left: 20px;">- ODER - • dem Zentralsystem eine Firma zugeordnet ist. 	29253
<p>Bei der Synchronisation von SAP R/3-Personalplanungsdaten, die erst zukünftig wirksam werden, werden einige Daten nicht eingelesen.</p> <p>Ursache: Die Funktion BAPI_EMPLOYEE_GETDATA wird immer mit dem aktuellen Tagesdatum ausgeführt. Damit werden Änderungen taggenau beachtet.</p> <p>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.</p>	29556
<p>Der Zielsystemabgleich zeigt in der Manager Webanwendung keine Informationen an.</p> <p>Workaround: Nutzen Sie den Manager, um den Zielsystemabgleich durchzuführen.</p>	30271

Bekanntes Problem	Fehler ID
<p>Bei Bestellung eines Zugriffs auf ein Asset aus dem Bereich einer Zugriffsanforderungsrichtlinie, die für assetbasierten Sitzungszugriff vom Typ Benutzer angegeben konfiguriert ist, tritt im One Identity Safeguard folgender Fehler auf:</p> <p>400: Bad Request -- 60639: A valid account must be identified in the request.</p> <p>Die Bestellung wird im One Identity Manager abgelehnt und der Fehler in der Bestellung als Begründung angezeigt.</p>	796028, 30963
<p>Bei Inkonsistenzen in der SharePoint-Umgebung kann es passieren, dass bereits der Zugriff auf eine Eigenschaft einen Fehler verursacht. Der Fehler erscheint auch dann, wenn das Mapping der betroffenen Schemaeigenschaft deaktiviert wird.</p> <p>Ursache: Der SharePoint Konnektor lädt standardmäßig alle Objekteigenschaften in einen Cache.</p> <p>Lösung:</p> <ul style="list-style-type: none"> • Korrigieren Sie den Fehler im Zielsystem. - ODER - • Deaktivieren Sie den Cache in der Datei VI.Projector.SharePoint.<Version>.Host.exe.config. 	31017
<p>Wenn eine SharePoint Websitesammlung nur lesbar ist, kann das Serverfarmkonto die Schemaeigenschaften Owner, SecondaryContact und UserCodeEnabled nicht lesen.</p> <p>Workaround: Bei der Synchronisation werden für die Eigenschaften UID_SPSUserOwner und UID_SPSUserOwnerSecondary Leerwerte in die One Identity Manager-Datenbank geschrieben. In diesem Fall wird kein Ladefehler im Synchronisationsprotokoll aufgezeichnet.</p>	31904
<p>Wenn Datumsfelder in einer SAP R/3-Umgebung Werte enthalten, die kein gültiges Datums- oder Uhrzeitformat repräsentieren, kann der SAP-Konnektor diese Werte nicht lesen, da die Typkonvertierung scheitert.</p> <p>Lösung: Bereinigen Sie die fehlerhaften Daten.</p> <p>Workaround: Die Typkonvertierung kann deaktiviert werden. Voraussetzung dafür ist, dass auf dem Synchronisationsserver der SAP .Net Connector for .NET 4.8 on x64, mindestens Version 3.1.2.0 installiert ist.</p>	32149
<p>WICHTIG: Da mit diesem Workaround die Datumsprüfung komplett umgangen wird, sollte er nur genutzt werden, wenn keine andere Lösung umsetzbar ist.</p>	
<p>Um die Typkonvertierung zu deaktivieren</p>	

- 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.RfcGeneralConfigurati
    on, sapnco, Version=3.1.2.42, Culture=neutral,
    PublicKeyToken=50436dca5c7f7d23" />
</sectionGroup>
```
 - Eine neue Sektion:


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

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

Ursache:

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

Lösung:

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

Beispiel:

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

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

Der Google Workspace-Konnektor kann die Nutzerdaten von Google Applikationen vor dem Löschen eines Benutzerkontos nicht erfolgreich auf ein anderes Google Workspace Benutzerkonto übertragen. Der Transfer scheitert an den Nutzerdaten der Applikation Rocket. 33104

Workaround: Hinterlegen Sie in den erweiterten Einstellungen der Systemverbindung zu Google Workspace ein Nutzerdatentransfer XML. In diesem XML-Dokument schränken Sie die Liste der zu übertragenden Nutzerdaten ein. Führen Sie nur die Google Applikationen auf, deren Nutzerdaten Sie weiterhin benötigen. Ausführliche Informationen und ein Beispiel-XML finden Sie im *One Identity Manager Administrationshandbuch für die*

Bekanntes Problem	Fehler ID
<i>Anbindung einer Google Workspace-Umgebung.</i>	
<p>Wenn in der Schematypdefinition einer Schemaerweiterungsdatei für das SAP R/3-Schema ein <code>DisplayPattern</code> 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.</p>	33812
<p>Lösung: Lassen Sie <code>DisplayPattern</code> in der Schematypdefinition leer. Es wird automatisch der definierte Name des Objekts als Anzeigewert verwendet.</p>	
<p>Enthalten Zielsystemdaten nachgestellte Leerzeichen so gehen diese bei der Synchronisation in den One Identity Manager verloren. Jede weitere Synchronisation erkennt Datenänderungen und schreibt die betroffenen Werte immer wieder oder legt neue Objekte an, wenn diese Eigenschaften Teil der Object-Matching-Regel ist.</p>	33448
<p>Lösung: Nachgestellte Leerzeichen sollten bereits im Zielsystem vermieden werden.</p>	
<p>Der Prozess zur Provisionierung von Objektänderungen startet, bevor das Synchronisationsprojekt aktualisiert wurde.</p>	34903
<p>Lösung: Reaktivieren Sie den Prozess zur Provisionierung von Objektänderungen, nachdem der Prozess <code>DPR_Migrate_Shell</code> abgearbeitet wurde.</p>	
<p>Nach einem Update von <code>SAP_BASIS 7.40 SP 0023</code> auf <code>SP 0026</code> oder <code>SAP_BASIS 7.50 SP 0019</code> auf <code>SP 0022</code> kann sich der SAP R/3 Konnektor nicht mehr mit dem Zielsystem verbinden.</p>	34650
<p>Nach einer Aktualisierung von One Identity Manager Version 8.0 oder Version 8.1 auf One Identity Manager Version 8.2.1 oder höher, kann es vorkommen, dass PowerShell-Skripte, die auf das Az-PowerShell-Modul (<code>Import-Module Az</code>) verweisen, nicht funktionieren. In einer PowerShell, die auf demselben Host gestartet wird, funktionieren die Skripte ohne Fehler. Bei der Ausführung der Prozessfunktion <code>ExecuteScript</code> durch die Prozesskomponente <code>PowerShellComponentNet4</code> werden Fehlermeldungen protokolliert.</p>	37116
<p>Beispiel: Entry point was not found.</p>	
<p>Ursache: Mit One Identity Manager Version 8.2.1 oder höher wird eine Bibliothek <code>Azure.Core.dll</code> mit einer bestimmten Version mitgeliefert. Das kundenspezifische PowerShell-Skript hängt möglicherweise von einer neueren Version des Az-PowerShell-Moduls ab. Wenn der One Identity Manager Service das Skript ausführt, wird die lokal</p>	

Bekanntes Problem

Fehler ID

gespeicherte Azure.Core.dll verwendet, wodurch die Abhängigkeit unterbrochen wird.

Mögliche Workarounds: Prüfen Sie die Einsatzmöglichkeit der folgenden Workarounds hinsichtlich Eingabeparameter und Rückgabewert.

- Rufen Sie PowerShell als Unterprozess auf
Um einen PowerShell-Befehl aus dem aktuellen Prozess heraus auszuführen, starten Sie einen neuen PowerShell-Prozess direkt mit dem Befehlsaufruf.

```
pwsh -c 'Invoke-ConflictingCommand'
```
- Verwenden Sie die Prozesskomponente `CommandComponent` mit der Prozessfunktion `Execute`, um die PowerShell-Anwendung mit folgendem Befehlsaufruf zu starten.

```
powershell -c 'Invoke-ConflictingCommand'
```

Tabelle 14: Identity Management und Access Governance

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

Tabelle 15: Drittanbieter-Komponenten

Bekanntes Problem	Fehler ID
Die Installation des One Identity Manager Service mit Server Installer auf einem Windows Server funktioniert nicht, wenn die Einstellung File and	24784

Bekanntes Problem	Fehler ID
<p>Printer Sharing am Server deaktiviert ist. Auf einem Domänen-Controller ist diese Einstellung aus Sicherheitsgründen deaktiviert.</p>	
<p>Beim Verbinden mit einer Oracle Database kommt es sporadisch zu einem der folgenden Fehler: TNS-12516, TNS-12519 oder ORA-12520. Erneute Verbindungsversuche sind jedoch meist erfolgreich.</p> <p>Mögliche Ursache: Die Anzahl der gestarteten Prozesse erreicht das am Server konfigurierte Limit.</p>	27830
<p>In einem mehrseitigen Synchronisationsprotokoll kann nicht mit der Maus und mit den Pfeiltasten navigiert werden.</p> <p>Ursache: Die StimulReport.Net-Komponente der Firma Stimulsoft behandelt den Bericht als eine Seite.</p>	29051
<p>Gültiger CSS-Code verursacht einen Fehler unter Mono, wenn doppelte Schlüssel vorhanden sind. Weitere Informationen finden Sie unter https://github.com/mono/mono/issues/7455.</p>	762534, 762548, 29607
<p>Mitgliedschaften in Active Directory Gruppen vom Typ Universal in einer untergeordneten Domäne werden im Zielsystem nicht entfernt, wenn eines der folgenden Windows Updates installiert ist:</p> <ul style="list-style-type: none"> • Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 <p>One Identity ist derzeit nicht bekannt, ob weitere Windows Updates zu diesem Fehler führen können.</p> <p>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.</p>	30575
<p>Unter Umständen kommt es im Report Editor zur Verwendung der falschen Sprache in den Steuerelementen von Stimulsoft.</p>	31155
<p>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 <code>boolean</code> definiert wird), kann das in One Identity Manager zu verschiedenen Problemen führen.</p>	31998
<p>In bestimmten Active Directory/Microsoft Exchange-Topologien schlägt das Cmdlet <code>Set-Mailbox</code> mit folgendem Fehler fehl:</p>	33026

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

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

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

Mögliche Workarounds:

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

Schemaänderungen

Nachfolgend finden Sie eine Übersicht der Schemaänderungen von Version 9.2 zu Version 9.2.1.

Identity Management Basismodul

- Neue Spalten `QERVPersonAndAERoles.InheritInfo`, `QERVPersonAndAERoles.ObjectKeyAssignment`, `QERVPersonAndAERoles.ObjectKeyOrg` und `QERVPersonAndAERoles.UID_SourceColumn` zur verbesserten Abbildung von Verantwortlichkeiten.

Privileged Account Governance Modul

- Die Spalten `PAGAccGroup.AssetGroupingRule`, `PAGAccGroup.DirectoryAccountGroupingRule` und `PAGAccGroup.AssetAccountGroupingRule` wurden auf `nvarchar(max)` verlängert.

Modul SAP R/3 Compliance Add-on

- Neue Pflichtfelddefinition für die Spalte `SAPFunctionDetail.UID_SACTransactionType`.

Microsoft Exchange Modul

- Neue Tabelle EX0VCanSendAs zur Abbildung von Sendeberechtigungen.

Exchange Online Modul

- Die Spalte O3EMailbox.AdditionalResponse wurde auf nvarchar(max) verlängert.

Änderungen an Systemkonnektoren

Nachfolgend finden Sie eine Übersicht der geänderten Synchronisationsvorlagen und eine Übersicht aller bereitgestellten Patches von One Identity Manager Version 9.2 zu Version 9.2.1. Wenden Sie die Patches auf bestehende Synchronisationsprojekte an. Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 64.

Änderungen an Synchronisationsvorlagen

Nachfolgend finden Sie eine Übersicht der Synchronisationsvorlagen. Um Änderungen an Synchronisationsvorlagen in bestehende Synchronisationsprojekte zu übernehmen, werden Patches bereitgestellt. Weitere Informationen finden Sie unter [Patches für Synchronisationsprojekte](#) auf Seite 35.

Tabelle 16: Übersicht der Synchronisationsvorlagen und Patches

Modul	Synchronisationsvorlage	Art der Änderung
Modul Zielsystemsynchronisation	Automatic One Identity Manager Synchronization	keine
Azure Active Directory Modul	Azure Active Directory Synchronization	keine
	Azure Active Directory B2C tenant	keine
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 Synchro-	keine

Modul	Synchronisationsvorlage	Art der Änderung
	nization	
	Oracle E-Business Suite CRM data	keine
	Oracle E-Business Suite HR data	keine
	Oracle E-Business Suite OIM data	keine
Microsoft Exchange Modul	Microsoft Exchange 2013/2016/2019 Synchronization (v2)	keine
Google Workspace Modul	Google Workspace Synchronization	keine
LDAP Modul	AD LDS Synchronization	keine
	AD LDS Synchronization (version 2)	keine
	OpenDJ Synchronization	keine
	OpenDJ Synchronization (version 2)	keine
	Generic LDAP Synchronization (version 2)	keine
	Oracle DSEE Synchronization (version 2)	keine
Domino Modul	Lotus Domino Synchronization	keine
Exchange Online Modul	Exchange Online Synchronization (v2)	keine
Microsoft Teams Modul	Microsoft Teams (via Azure Active Directory)	keine
OneLogin Modul	OneLogin Domain Synchronization	keine
Privileged Account Governance Modul	One Identity Safeguard Synchronization	keine
SAP R/3 Benutzermanagement-Modul	SAP R/3 Synchronization (Base Administration)	keine
	SAP R/3 (CUA subsystem)	keine
Modul	SAP R/3 BW	keine

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

Patches für Synchronisationsprojekte

Nachfolgend finden Sie eine Liste aller Patches für Synchronisationsprojekte, die im One Identity Manager 9.2.1 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 64.

Tabelle 17: Patches für Microsoft Exchange

Patch ID	Patch	Beschreibung	Fehler ID
VPR#37274	Anpassen der Beschreibungen der Variablen	<p>Passt die Beschreibungen der Variablen für Synchronisationsprojekte an.</p> <p>Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.</p>	37274

Tabelle 18: Patches für SharePoint Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#37272	Setzt Filter für die Schemaeigenschaften vrtLcid und vrtLanguage	Setzt Systemfilter in den Schemaeigenschaften vrtLcid und vrtLanguage in den Mappings Site, Web und WebTemplate.	37272

Tabelle 19: Patches für SAP R/3 Berechtigungsobjekte

Patch ID	Patch	Beschreibung	Fehler ID
VPR#37380	Neue Mappings und Synchronisationsschritte für die partitionierte Verarbeitung von SAP Berechtigungsobjekten	Fügt neue Schemaklassen, Mappings und Synchronisationsschritte zur partitionierten Verarbeitung von ProfileHasAuthObjectField-Objekten ein. Die neuen Synchronisationsschritte sind standardmäßig deaktiviert.	37380, 438884

Tabelle 20: Patches für die SCIM-Schnittstelle (im Modul Universal Cloud Interface)

Patch ID	Patch	Beschreibung	Fehler ID
ADO#444262	Neue Variable zur Konfiguration der Übertragung der Zugangsdaten	Fügt die Variable dprauthoauthusebody ins Standardvariablenset und die Verbindungsparameter ein. Damit kann die Übertragung der Zugangsdaten in Header oder Body konfiguriert werden. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	444262

Patches in One Identity Manager Version 9.2

Tabelle 21: Allgemeine Patches

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36755	Deaktivierung des Synchronisationspuffers für die Zentraldatenbank	Deaktiviert den Synchronisationspuffer für verschiedene virtuelle Schemaeigenschaften im Schema der Zentraldatenbank in Synchronisationsprojekten für die Systemsynchronisation.	36755

Patch ID	Patch	Beschreibung	Fehler ID
	Meilenstein 9.2	Meilenstein für den Kontext DPR .	
	Meilenstein 9.2	Meilenstein für den Kontext One Identity Manager .	

Tabelle 22: Patches für Azure Active Directory

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

Patch ID	Patch	Beschreibung	Fehler ID
		Auf diese Schemaeigenschaften kann nur zugegriffen werden, wenn eine Azure Active Directory-Premium-Lizenz vorhanden ist.	
VPR#35769	Ermöglicht die Abbildung von Dienstprinzipalen als Eigentümer von Dienstprinzipalen	Erweitert den Mitgliederfilter der Property-Matching-Regel <code>vrtOwners_Owners</code> im Mapping <code>ServicePrincipal</code> auf Dienstprinzipale. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	35769
VPR#35513	Unterstützung von RBAC und PIM Funktionen	Erweitert die Synchronisationskonfiguration für die Synchronisation von Objekte für die rollenbasierte Zugriffssteuerung (RBAC) und das Privileged Identity Management (PIM). Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	35513
	Meilenstein 9.2	Meilenstein für den Kontext Azure Active Directory .	

Tabelle 23: Patches für Active Directory

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

Tabelle 24: Patches für Active Roles

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

Tabelle 25: Patches für Microsoft Exchange

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

Tabelle 26: Patches für HCL Domino

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36087	Mapping der Roaming-Eigenschaften von Benutzerkonten	Erweitert das Mapping Person zur Abbildung der Roaming-Eigenschaften von Benutzerkonten. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36087
VPR#36831	Entfernen von	Entfernt Quotas für die Methode Delete	36831

Patch ID	Patch	Beschreibung	Fehler ID
	Quotas zum Löschen von Objekten	object aus den Synchronisationsschritten CertifierRequest und AdminRequest.	
	Meilenstein 9.2	Meilenstein für den Kontext HCL Domino .	

Tabelle 27: Patches für Exchange Online

Patch ID	Patch	Beschreibung	Fehler ID
VPR#35780	Neue Property-Mapping-Regeln zur Abbildung eines hierarchischen Adressbuchs	Fügt neue Property-Mapping-Regeln in verschiedene Mappings ein, um ein hierarchisches Adressbuch abzubilden. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	35780
	Meilenstein 9.2	Meilenstein für den Kontext Exchange Online .	

Tabelle 28: Patches für SharePoint Online

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

Tabelle 29: Patches für Privileged Account Management

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36044	Unterstützung von One Identity Safeguard Partitionen	Erweitert die Synchronisationskonfiguration zur Unterstützung von One Identity Safeguard Partitionen.	36044
VPR#36315	Abbildung der One Identity Safeguard Prüfprotokolle	Erweitert die Synchronisationskonfiguration, um die One Identity Safeguard Prüfprotokolle (AuditLog) einzulesen.	36315

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36617	Unterstützung für One Identity Safeguard 7.2 und 7.3	Erweitert die Synchronisationskonfiguration zur Unterstützung der Versionen 7.2 und 7.3 von One Identity Safeguard.	36617, 36943
	Meilenstein 9.2	Meilenstein für den Kontext Privileged Account Management .	

Tabelle 30: Patches für SAP R/3

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

Tabelle 31: Patches für SAP R/3 Berechtigungsobjekte

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

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

Patch ID	Patch	Beschreibung	Fehler ID
VPR#36376	Neue Variable zur Konfiguration der Listeneinstellungen	Fügt eine Variable zur Konfiguration der Elemente pro Seite bei Anfragen für die Objektliste in das Standardvariablenset und die Verbindungsparameter ein. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	36376
VPR#36985	Korrektur von Schemae-	Speichert die Namen der Erwei-	36985

Patch ID	Patch	Beschreibung	Fehler ID
	rweiterungen	terungen von Schematypen im Schema. Dieser Patch wird während der Aktualisierung von One Identity Manager automatisch angewendet.	
	Meilenstein 9.2	Meilenstein für den Kontext SCIM .	

Tabelle 33: Patches für Unix

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

Abgekündigte Funktionen

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

- Der Domino-Konnektor unterstützt die Synchronisation folgender Umgebungen nicht mehr:
 - IBM Domino Server Version 8, 9 und 10
 - HCL Domino Server Version 11
 - IBM Notes Client Version 8.5.3 oder 10.0
 - HCL Notes Client Version 11.0.1 und 12.0
- Folgende Skripte wurden entfernt.

- VI_GetValueOfObject
- VID_GetValueOfDialogObject
- VI_ITDataFromOrg
- VI_AE_ITDataFromOrg
- VI_GetOrgUnitFromCertifier
- VI_ConvertDNToCanonicalName
- VI_PersonAuto_LDAP
- VI_PersonAuto_ADS
- VI_PersonAuto_EBS
- VI_PersonAuto_Notes
- VI_PersonAuto_SAP
- VI_PersonAuto_SharePoint_SPSUser
- VI_GetAttestationObject
- VI_GetDNParser
- TSB_Find_And_Use_Linked_Account_For_AccountDef
- Folgende Konfigurationsparameter wurden entfernt.
 - TargetSystem | ADS | DBDeleteOnError
 - TargetSystem | ADS | VerifyUpdates
 - TargetSystem | EBS | DBDeleteOnError
 - TargetSystem | NDO | VerifyUpdates
 - TargetSystem | SAPR3 | DBDeleteOnError
 - TargetSystem | SAPR3 | VerifyUpdates
 - TargetSystem | SharePoint | DBDeleteOnError
- Die Gruppierung von Formulardefinitionen über ein Basisformular für Formularfolgen wird nicht mehr unterstützt.

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

- Folgende Funktionen werden für den One Identity Manager Service zukünftig nicht mehr unterstützt.
 - FileJobProvider
 - FileJobDestination
 - FileJobGate
 - FTPJobProvider
 - FTPJobDestination
 - HTTPJobProvider

- HTTPJobDestination
- HTTPJobGate
- Der Web Designer und die Web Designer-basierten Webanwendungen werden zukünftig nicht mehr unterstützt. Verwenden Sie die HTML-Webanwendungen, die über den API Server bereitgestellt werden.
- Die Tabelle PersonPasswordHistory wird in zukünftigen Versionen entfernt.
- Folgende Skripte sind als veraltet gekennzeichnet. Bei der Kompilierung wird eine entsprechende Warnung ausgegeben.
 - VI_AE_BuildCentralAccount
 - VI_AE_BuildCentralAccountGlobalUnique
 - VI_BuildInternalName
 - VI_AE_CreatedefaultMailAddress
 - VI_AE_BuildCentralSAPAccount
- Im Simulationsmodus im Manager wird die Verarbeitung von DBQueue Prozessor-Aufträgen, wie beispielsweise die Neuberechnung von Complianceregeln, zukünftig nicht mehr unterstützt. Dies betrifft die Plugins **Identity Audit Simulation** und **Identity Audit Simulationsauswertung** sowie den Bericht **VID_DatabaseSimulationResult_with_Compliance_Export**.
- Ab One Identity Manager Version 9.3 wird die Version SQL Server 2019 für die One Identity Manager-Datenbank nicht mehr unterstützt. Die Version SQL Server 2022 wird weiterhin unterstützt.
- Die Synchronisation mit Microsoft Exchange 2013 wird zukünftig nicht mehr unterstützt.
- Die Synchronisation mit SharePoint 2013 wird zukünftig nicht mehr unterstützt.
- Die Prozesskomponente PowerShellComponent wird zukünftig nicht mehr unterstützt. Verwenden Sie die Prozesskomponente PowershellComponentNet4.
- Der Container-Support für Windows Server 2016 wird für zukünftige Versionen abgekündigt.

Systemanforderungen

Stellen Sie vor der Installation von One Identity Manager 9.2.1 sicher, dass Ihr System den nachfolgenden minimalen Hardware- und Systemanforderungen entspricht.

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

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

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

Unterstützte Datenbanksysteme

One Identity Manager unterstützt folgende Datenbanksysteme:

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

Minimalanforderungen für den Einsatz von SQL Server als Datenbankserver

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

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung (nicht-produktiv) 16 physische Kerne mit 2.5 GHz+ Taktung (produktiv) HINWEIS: Aus Performancegründen wird der Einsatz von 16 physischen Kernen empfohlen.
Arbeitsspeicher	16 GB+ RAM (nicht-produktiv) 64 GB+ RAM (produktiv)
Freier Festplattenspeicher	100 GB
Betriebssystem	Windows Betriebssysteme <ul style="list-style-type: none"> • Beachten Sie die Anforderungen von Microsoft für die eingesetzte SQL Server Version. UNIX und Linux Betriebssysteme

- Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für SQL Server Datenbanken.

Software

Unterstützt werden die Versionen:

- SQL Server 2019 Standard Edition (64-Bit) mit aktuellem kumulativen Update
- SQL Server 2022 Standard Edition (64-Bit) mit aktuellem kumulativen Update

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

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

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

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

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

Anforderungen an eine verwaltete Instanz in Azure SQL-Datenbank

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

Minimalanforderungen für Clients

Auf den Clients sind die folgenden Systemvoraussetzungen zu gewährleisten.

Prozessor	4 physische Kerne mit 2 GHz+ Taktung
Arbeitsspeicher	4 GB+ RAM
Freier Festplattenspeicher	1 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: <ul style="list-style-type: none">• Windows 11 (x64)• Windows 10 (32-Bit oder 64-Bit) mindestens Version 1511
Zusätzliche Software	<ul style="list-style-type: none">• Microsoft .NET Framework Version 4.8 oder höher• Microsoft Edge WebView2
Unterstützte Browserversionen	<ul style="list-style-type: none">• 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 Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: <ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016• Windows Server 2012 R2• Windows Server 2012

	Linux Betriebssysteme
	<ul style="list-style-type: none"> Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden.
Zusätzliche Software	Windows Betriebssysteme
	<ul style="list-style-type: none"> Microsoft .NET Framework Version 4.8 oder höher <p>HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers.</p>
	Linux Betriebssysteme
	<ul style="list-style-type: none"> Mono 6.10 oder höher

Minimalanforderungen für Webserver

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

Prozessor	4 physische Kerne mit 1.65 GHz+Taktung
Arbeitsspeicher	4 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme
	Unterstützt werden die Versionen:
	<ul style="list-style-type: none"> Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012
	Linux Betriebssysteme
	<ul style="list-style-type: none"> Linux Betriebssystem (64-Bit), welches vom Mono Projekt unterstützt wird oder Docker-Images, die vom Mono Projekt bereitgestellt werden. Beachten Sie die Minimalanforderungen des Betriebssystemherstellers für Apache HTTP Server.
Zusätzliche Software	Windows Betriebssysteme
	<ul style="list-style-type: none"> Microsoft .NET Framework Version 4.8 oder höher

- Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.8 und den Role Services:
 - Web Server > Common HTTP Features > Static Content
 - Web Server > Common HTTP Features > Default Document
 - Web Server > Application Development > ASP.NET
 - Web Server > Application Development > .NET Extensibility
 - Web Server > Application Development > ISAPI Extensions
 - Web Server > Application Development > ISAPI Filters
 - Web Server > Security > Basic Authentication
 - Web Server > Security > Windows Authentication
 - Web Server > Performance > Static Content Compression
 - Web Server > Performance > Dynamic Content Compression

Linux Betriebssysteme

- NTP - Client
- Mono 6.10 oder höher
- Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
 - mod_mono
 - rewrite
 - ssl (optional)

Minimalanforderungen für Anwendungsserver

Zur Installation des Anwendungsservers sind die folgenden Systemvoraussetzungen zu gewährleisten.

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	8 GB RAM
Freier	40 GB

Festplattenspeicher

Betriebssystem

Windows Betriebssysteme

Unterstützt werden die Versionen:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Linux Betriebssysteme

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

Zusätzliche Software

Windows Betriebssysteme

- Microsoft .NET Framework Version 4.8 oder höher
- Microsoft Internet Information Service 10 oder 8.5 oder 8 oder 7.5 oder 7 mit ASP.NET 4.8 und den Role Services:
 - Web Server > Common HTTP Features > Static Content
 - Web Server > Common HTTP Features > Default Document
 - Web Server > Application Development > ASP.NET
 - Web Server > Application Development > .NET Extensibility
 - Web Server > Application Development > ISAPI Extensions
 - Web Server > Application Development > ISAPI Filters
 - Web Server > Security > Basic Authentication
 - Web Server > Security > Windows Authentication
 - Web Server > Performance > Static Content Compression
 - Web Server > Performance > Dynamic Content Compression

Linux Betriebssysteme

- NTP - Client
- Mono 6.10 oder höher
- Apache HTTP Server 2.0 oder 2.2 mit folgenden Modulen:
 - mod_mono
 - rewrite
 - ssl (optional)

Unterstützte Datensysteme

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

Tabelle 34: 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. 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

Konnektor	Unterstützte Datensysteme
Active Directory Konnektor	<p data-bbox="560 264 836 293"> Konnektors nutzen.</p> <p data-bbox="560 320 1378 450">Active Directory, welches mit Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 und Windows Server 2022 ausgeliefert wird.</p>
Microsoft Exchange Konnektor	<ul data-bbox="611 477 1358 651" style="list-style-type: none"> • Microsoft Exchange 2013 mit kumulativem Update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 mit kumulativem Update 1 • MicrosoftExchange Hybrid-Umgebungen
SharePoint Konnektor	<ul data-bbox="611 674 1158 848" style="list-style-type: none"> • SharePoint 2013 • SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
SAP R/3 Konnektor	<ul data-bbox="611 871 1378 1261" style="list-style-type: none"> • SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55, 7.56, 7.57, 7.58 und 7.69 • SAP ECC 5.0 und 6.0 • SAP S/4HANA On-Premise-Edition 1.0 und 2.0 ab SAP BASIS 7.40 SR 2 und 7.50 (auch für Installationen mit SAP BASIS 7.53) • SAP S/4HANA Cloud 2022 und 2023 mit SAP BASIS 7.57 und 7.58
Unix Konnektor	<p data-bbox="560 1283 1358 1382">Unterstützt werden die gängigsten Unix und Linux Derivate. Weitere Informationen finden Sie in den Spezifikationen für One Identity Authentication Services.</p>
Domino Konnektor	<ul data-bbox="611 1404 1358 1520" style="list-style-type: none"> • HCL Domino Server Version 12 und 14 • HCL Notes Client Version 12.0.1 (nur 64-Bit-Variante) und 14.0 <p data-bbox="560 1543 1358 1606">Für HCL Domino Server und HCL Notes Client wird die selbe Hauptversion eingesetzt.</p>
Generischer Datenbankkonnektor	<ul data-bbox="611 1628 863 1803" style="list-style-type: none"> • SQL Server • Oracle Database • SQLite • MySQL

Konnektor	Unterstützte Datenysteme
	<ul style="list-style-type: none"> • DB2 (LUW) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe Konnektoren	<ul style="list-style-type: none"> • RACF • IBM i • CA Top Secret • CA ACF2
PowerShell Konnektor	<ul style="list-style-type: none"> • PowerShell Version 3 oder höher
Active Roles Konnektor	<ul style="list-style-type: none"> • Active Roles 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.5, 7.5.2, 7.5.3, 7.6, 8.0, 8.1.1, 8.1.3 und 8.1.5
Azure Active Directory Konnektor	<ul style="list-style-type: none"> • Microsoft Azure Active Directory <p>HINWEIS: Die Synchronisation von Azure Active Directory Mandanten in nationalen Cloud-bereitstellungen mit dem Azure Active Directory Konnektor wird nicht unterstützt.</p> <p>Dies betrifft:</p> <ul style="list-style-type: none"> • Microsoft Cloud for US Government (L5) • Microsoft Cloud Germany • Azure Active Directory und Microsoft 365 betrieben von 21Vianet in China <p>Weitere Informationen finden Sie auch unter https://support.oneidentity.com/KB/312379.</p> <ul style="list-style-type: none"> • Microsoft Teams
SCIM Konnektor	<p>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.</p>
Exchange Online Konnektor	<ul style="list-style-type: none"> • Microsoft Exchange Online
Google Workspace Konnektor	<ul style="list-style-type: none"> • Google Workspace
Oracle E-Business Suite	<ul style="list-style-type: none"> • Oracle E-Business Suite Version 12.1, 12.2 und 12.2.10

Konnektor	Unterstützte Datensysteme
Konnektor	
SharePoint Online Konnektor	<ul style="list-style-type: none"> • Microsoft SharePoint Online
One Identity Safeguard Konnektor	<ul style="list-style-type: none"> • One Identity Safeguard Version 6.0, 6.7, 6.13, 7.0, 7.1, 7.2, 7.3, 7.4 und 7.5 <p>Für die im einzelnen unterstützten Versionen finden Sie auf dem One Identity Manager Installationsmedium im Verzeichnis Modules\PAG\dvd\AddOn\safeguard-ps das passende PowerShell Modul. Versionen, für die kein PowerShell Modul auf dem One Identity Manager Installationsmedium vorhanden ist, werden nicht unterstützt.</p>

Long Term Support (LTS) und Feature Releases

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

Long Term Support (LTS)

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

Feature Releases

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

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

Tabelle 35: Vergleich von Long Term Support (LTS) Release und Feature Release

Kategorie	Long Term Support (LTS) Release	Feature Release
Release-Frequenz	Alle 36 Monate (umfasst Fehlerbehebungen und sicherheitsrelevante Aktualisierungen).	Ungefähr alle 12 Monate (umfasst Fehlerbehebungen und sicherheitsrelevante

Kategorie	Long Term Support (LTS) Release	Feature Release
		Aktualisierungen).
Dauer uneingeschränkter Support	36 Monate	18 Monate
Dauer begrenzter Support	12 Monate (nach Ablauf des uneingeschränkten Supports)	6 Monate (nach Ablauf des uneingeschränkten Supports)
Versionierung	Alle Versionen, bei denen die zweite Ziffer 0 ist. Zum Beispiel: 9.0.0 (9.0.1, 9.0.2, ...), 10.0.0, 11.0.0, und so weiter.	Alle Versionen, bei denen die zweite Ziffer nicht 0 ist. Zum Beispiel: 9.1.0 (9.1.1, 9.1.2), 9.2, 9.3, und so weiter.
Verfügbarkeit von Service Packs zwischen Releases	Ungefähr alle 6 Monate werden kumulative Updates (CUs) für jede LTS-Version erwartet.	Alle 6 Monate werden Patch Releases (Service Pack) für jeden derzeit unterstützten Feature Release erwartet.
Kriterien für die Bereitstellung von Hotfixes für LTS außerhalb eines kumulativen Aktualisierungszyklus	<ul style="list-style-type: none"> • Das Produkt funktioniert nach der Installation des letzten CUs nicht mehr und der Kunde kann nicht warten, bis das nächste CU verfügbar ist. • Das Produkt funktioniert nicht/ist nicht funktionsfähig, was zu einem Produktionsausfall/einem schwerwiegenden Problem führt. • Eine sicherheitsrelevante Korrektur wird dringend benötigt, um eine Schwachstelle zu beheben. • Es werden keine Korrekturen zur Umsetzung einer Verbesserung außerhalb des kumulativen Aktualisierungszyklus herausgeben. 	

Details zu den Releases finden Sie unter [Product Life Cycle](#).

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

Wechsel zwischen LTS-Versionen und Feature Release-Versionen

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

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

Patches

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

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

Weitere Informationen finden Sie im Knowledge Artikel [4372133](#).

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

Häufig gestellte Fragen (FAQs)

Was ist langfristiger Support (LTS)?

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

Was sind die Vorteile einer LTS-Version?

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

Was sind die Nachteile einer LTS-Version?

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

Dauer einer LTS-Version

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

Wie erfolgt der Wechsel zur LTS-Supportoption?

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

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

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

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

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

Produktlizenzierung

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

Upgrade und Installationsanweisungen

Um One Identity Manager 9.2.1 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 9.2.1 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 9.2.1 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 mit der Version 9.2.1 sowie der Aktualisierung einer One Identity Manager-Datenbank von Version 8.0.x auf die Version 9.2.1 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 9.2.1 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.

- 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*.
- Nutzen Sie das SDK-Skript `Modules\QBM\dvd\AddOn\SDK\SQLSamples\MSSQL2K\SDK_Remove_Rights_on_msdb.sql` um nicht mehr benötigte Berechtigungen für die msdb-Datenbank zu entfernen.
- Es ist nicht empfohlen, gleichzeitig eine Aktualisierung der vorhandenen Module auf eine neue One Identity Manager-Version und eine Installation zusätzlicher Module auszuführen. Unter Umständen können Abhängigkeiten zwischen Modulen nicht korrekt hergestellt werden. Aktualisieren Sie zuerst die vorhandenen Module auf die neue One Identity Manager-Version. Anschließend starten Sie den Configuration Wizard erneut und installieren die zusätzlichen Module.
- Bevor Sie eine Datenbank mit der One Identity Manager Version 8.2.x auf eine Version 9.2.x aktualisieren, führen Sie das Skript `QBM\Database\MSSQL\040Procedures\QBM_GCommon2\QBM_PWriteDialogJournal.sql` in einem geeigneten Programm zur Ausführung von SQL-Abfragen aus.

Aktualisieren des One Identity Manager auf Version 9.2.1

WICHTIG: Beachten Sie die [Hinweise zur Aktualisierung des One Identity Manager](#) auf Seite 58.

Um eine bestehende One Identity Manager Installation auf die Version 9.2.1 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.
 - c. Klicken Sie **Installieren**.

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

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

3. Beenden Sie den One Identity Manager Service auf dem Aktualisierungsserver.
4. Erstellen Sie eine Sicherung der One Identity Manager-Datenbank.
5. Prüfen Sie, ob der Kompatibilitätsgrad der Datenbank auf den Wert **150** eingestellt ist und passen Sie die Wert bei Bedarf an.
6. Führen Sie die Schemaaktualisierung der One Identity Manager-Datenbank aus.
 - Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation und folgen Sie den Anweisungen.

Verwenden Sie für die Aktualisierung des One Identity Manager Schemas mit dem Configuration Wizard einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.

- Verwenden Sie denselben Benutzer, den Sie auch für die initiale Schemainstallation verwendet haben.
- Haben Sie bei der Schemainstallation einen administrativen Benutzer erstellt, dann verwenden Sie diesen Benutzer.
- Haben Sie zur Schemainstallation einen Benutzer mit Windows-

Authentifizierung gewählt, dann müssen Sie diesen Benutzer zur Aktualisierung verwenden.

HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 9.2.1 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.
 - c. Klicken Sie **Installieren**.
Der Installationsassistent wird gestartet.
 - d. Folgen Sie den Installationsanweisungen.

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

8. Prüfen Sie die Anmeldeinformationen des One Identity Manager Service. Geben Sie das zu verwendende Dienstkonto an.
9. Starten Sie den One Identity Manager Service auf dem Aktualisierungsserver.
10. Aktualisieren Sie weitere Installationen auf Arbeitsstationen und Servern.
Für die Aktualisierung vorhandener Installationen können Sie das Verfahren der automatischen Softwareaktualisierung einsetzen.

Um Synchronisationsprojekte auf die Version 9.2.1 zu aktualisieren

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

HINWEIS: Einige Patches werden automatisch angewendet. Dafür wird ein Prozess in die Jobqueue eingestellt, der alle vorhandenen Synchronisationsprojekte migriert. Damit der Prozess ausgeführt werden kann, muss der

| One Identity Manager Service auf allen Synchronisationsservern gestartet sein.

- Prüfen Sie, ob der Prozess DPR_Migrate_She11 erfolgreich ausgeführt wurde.
Wenn ein Patch nicht angewendet werden konnte, beispielsweise weil das Zielsystem nicht erreichbar war, können Sie diesen Patch nachträglich manuell anwenden.

Weitere Informationen finden Sie unter [Anwenden von Patches für Synchronisationsprojekte](#) auf Seite 64.

Um einen Anwendungsserver auf die Version 9.2.1 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 9.2.1 zu aktualisieren

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

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

Um einen API Server auf die Version 9.2.1 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 9.2.1 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 Änderungen aus der Version 9.2.1 in Ihre HTML-Anwendungen zu übernehmen

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

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

4. Prüfen Sie, ob Ihre HTML-Anwendungen noch ordnungsgemäß funktionieren.
5. Stellen Sie die neue Version Ihrer HTML-Anwendungen bereit.

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

Um die Manager-Webanwendung auf die Version 9.2.1 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 Bearbeitungsberechtigungen auf das Installationsverzeichnis der Manager-Webanwendung. Prüfen Sie, ob die entsprechenden Berechtigungen vorhanden sind.

Anwenden von Patches für Synchronisationsprojekte

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

Bevor Sie einen Patch anwenden

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

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

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

Um Patches anzuwenden

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie das Menü **Bearbeiten > Synchronisationsprojekt aktualisieren**.
3. Wählen Sie im Bereich **Verfügbare Patches** die Patches aus, die angewendet werden sollen. Mehrfachauswahl ist möglich.
Im Bereich **Details - Installationszusammenfassung** werden die Patches in der Reihenfolge angezeigt, in der sie angewendet werden.
4. Klicken Sie **Ausgewählte Patches anwenden**.
5. Wenn Benutzereingaben angefordert werden, erfassen Sie die benötigten Daten.
6. Prüfen Sie anhand des Patchprotokolls, ob kundenspezifische Anpassungen nachbearbeitet werden müssen.
7. Falls erforderlich, überarbeiten Sie die kundenspezifischen Anpassungen in der Synchronisationskonfiguration.
8. Führen Sie eine Konsistenzprüfung durch.
9. Simulieren Sie die Synchronisation.
10. (Optional) Aktivieren Sie das Synchronisationsprojekt.
11. Speichern Sie die Änderungen.

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

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

Siehe auch:

- [Änderungen an Synchronisationsvorlagen](#) auf Seite 33
- [Patches für Synchronisationsprojekte](#) auf Seite 35

Prüfen der erfolgreichen Installation

Um festzustellen, ob die Version installiert ist

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

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

Die Versionsnummer 2023.0009.0002.0100 für alle Module und die Anwendungsversion 9.2 v92-252751 weisen darauf hin, dass diese Version installiert ist.

Zusätzliche Ressourcen

Zusätzliche Informationen sind verfügbar unter:

- [One Identity Manager Support](#)
- [One Identity Manager Online-Dokumentation](#)
- [One Identity Manager Community](#)
- [One Identity Manager Trainingsportal](#)

Weltweite Verwendung

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

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

Diese Version ist in folgenden Sprachen lokalisiert: Deutsch

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

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Copyright 2024 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.



Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter <http://www.OneIdentity.com/legal/patents.aspx>.

Marken

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken, besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal/trademark-information.aspx. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

Legende

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