One Identity Manager

These release notes provide information about the One Identity Manager release version 10.0. You will find all the modifications since One Identity Manager version 9.3.1 listed here.

One Identity Manager 10.0 is a major release with new functionality and enhanced behavior. See New features and Enhancements.

If you are updating a One Identity Manager version older than One Identity Manager 9.3.1, read the release notes from the previous versions as well. Release notes and the release notes about the additional modules based on One Identity Manager technology can be found under One Identity Manager Publications.

One Identity Manager documentation is available in both English and German. The following documents are only available in English:

- Password Synchronization Configuration with the Password Capture Agent
- Setting Up the LDAP Connector for CA Top Secret
- Setting Up the LDAP Connector for IBM RACF
- Setting Up the LDAP Connector for IBM i
- Setting Up the LDAP Connector for CA ACF2
- One Identity Manager REST API
- One Identity Manager Object Layer Documentation
- One Identity Manager Composition API Object Model Documentation
- Secure Password Extension Configuration

About One Identity Manager

One Identity Manager simplifies the process of managing user identities, access permissions, and security policies. It gives control over identity management and access decisions to your organization, freeing up the IT team to focus on their core competence.

The One Identity Manager enables you to realize Access Governance demands cross-platform within your entire company. One Identity Manager is based on an automationoptimized architecture and, unlike other “traditional” solutions, addresses major identity and access management challenges in a fraction of the time, complexity, and expense.

One Identity Starling

Initiate your subscription within your One Identity on-prem product and join your on-prem solutions to our One Identity Starling cloud platform. Giving your organization immediate access to a number of cloud-delivered microservices, which expand the capabilities of your One Identity on-prem solutions. We will continuously make available new products and features to One Identity Starling.

For a free trial of our One Identity Starling offerings and to get the latest product feature updates, visit https://www.cloud.oneidentity.com.

New features

New features in One Identity Manager 10.0:

General

- One Identity Manager is now based on .NET 10.

  Ensure that .NET 10 is installed on all workstations and servers. For more information, see System requirements.

  Some functions are no longer supported. For more information, see Deprecated features.
- Online documentation is now used by default in the help system. It is still possible to install the help system locally. New machine roles are provided to do this.
- Support for loading configuration options for secrets from AWS Secrets Manager.
- The **TargetSystem | LDAP | AuthenticationV2 | CertificateRevocationMode** configuration parameter can be used to specify how certificate revocation checks are applied when logging in with LDAP-based authentication modules.
- Successful logins, failed login attempts, and logouts can all be logged. The messages can be sent to a syslog server. Logins and logouts are stored in the `QBMLoginAudit` table. The new **Common | Journal | LoginAudit | LifeTimeFailure**, **Common | Journal | LoginAudit | LifeTimeSuccess** and **Common | Journal | LogoffAudit | LifeTimeLogoff** configuration parameters can be used to specify the retention times for messages.

  > **NOTE:** For existing installations:
  >
  > This feature replaces the previous auditing of logins and logouts in the system journal (table `DialogJournal`). If necessary, adapt custom uses of this data, in reports or processes for example.
- Support for ECDA certificates as session certificates in the application server.

- SIEM messages can now be created for all changes to data in selected tables. A selection of predefined SIEM message definitions is supplied and can be enabled according to customer requirements.
- A minimum value and a maximum value can be defined for columns.
- New column format that enforces CRLF line endings to handle line break characters better in multi-line content fields.
- A separate limit for batch processing can be set for DBQueue Processor tasks.
- Standalone assemblies without dependencies can be referenced directly in scripts using the **#A** directive.
- New **Clear solution folders after build** option in the Database Compiler and new `/CleanUpAfterBuild` option in the `DBCompilerCMD.exe` command line program to clean up the AssemblyCache directory after compilation.
- The controls for the user interface have been reworked. Selection of dynamic entries, input of encrypted values and multiple values have been improved. A slim creation function can be configured to enable new referenced objects to be entered quickly on main data forms.
- To prevent dependency conflicts in future updates and hotfixes, some components will be isolated in separate deployment units with their own dependencies. Some process components and PowerShell-based connectors are run in a separate process and communicate via a defined protocol.

  The new **Isolated** exe type allows process components to be started in a runnable component (`.exe`).

  > **NOTE:** Currently only the `PowershellComponentNet4` process component supports the **Isolated** exe type. The exe type may not be changed and cannot be used for any other process component.

API configuration

- New machine roles have been introduced that can be used to control which APIs and web applications are available on an installed API Server. Machine roles can be selected and subsequently changed in the Web Installer.
- In the API Server, API methods that make object changes now return the process ID for process tracking in their response.
- Navigate to other web applications using the application switcher on the login page and in the header area of each web application. In the Administration Portal, use the **Applications can be switched (PortalSwitcherEnabled)** and **Excluded applications for application switch (ApplicationSwitchFilter)** configuration keys to configure this feature. The overview page of available web applications has been removed.
- For OAuth authentication, the name of the identity provider is now displayed on the web application login pages. This can be configured in the Administration Portal using the **Display identity provider name for OAuth login (UseIdentityProviderNameForOAuth)** configuration key.

- In the Administration Portal, it is now possible to use the **Custom CSS code (CustomCss)** configuration key to store your own CSS code, which is used for web applications.
- In the Administration Portal, the **Requests with unresolvable rule violations can be submitted (AllowRequestsWithNonResolvableViolations)** and **Role-inherent compliance check for assignment requests (CheckRoleInherentCompliance)** configuration keys are now available for further configuration of the shopping cart check.
- In the Administration Portal, API projects can now be excluded from loading when the API Server starts using the **Excluded API projects (ExcludedApiProjects)** configuration key. The APIs of these API projects are then no longer provided by the API Server.
- In the Administration Portal, you can now use the **Foreign key columns linked to candidate API methods (configurableFkColumns)** configuration key to specify the foreign key columns for which you want to create different candidate API methods.
- In the Administration Portal, it is now possible to specify which table properties can be used in custom filters. To do this, you must create a new configuration key for the relevant table and then configure the **Filterable properties** configuration key as required.
- Log messages in ASP.NET Core are forwarded to the NLog interface.

HTML5 web development

- Changes made by an API method can now be assigned to a change label using the **taguid** parameter.
- Static files (such as image files) can be uploaded with the Software Loader and retrieved directly from the API Server using a URL.

HTML5 web applications

- The new Intelligent Query Chatbot Module (IQC) allows Web Portal users to ask questions about the current data, these are sent to a large language model via an API and then answered. This module is not selected by default during installation or updating. To use the Intelligent Query Chatbot in the Web Portal, users require the **ApiServer_GenAIChatbot** program function.

  > **IMPORTANT:** This feature is governed by the Generative AI Terms of Use.

  > **NOTE:** One Identity recommends that you do not enter any personal data or confidential company information in the prompt.

  > **NOTE:** AI-generated content may not be accurate.

- Members of the **Basic roles | Operational support | System administrators** application role can now view and edit selected basic system configuration data in the Operations Support Web Portal.

  - Configuration parameters for system configuration can be edited.
  - Templates can be selected from the configuration library.
  - SIEM message definitions can be enabled.
  - Schedules can be edited.
  - Authentication modules can be enabled or disabled.
  - A revised wizard for integrating an identity provider is now available.

- The **Process Archive** page for archived processes has been added to the Operations Support Web Portal.
- It is now possible to configure synchronization between the One Identity Manager database and a target system by editing synchronization projects and startup sequences in the Operations Support Web Portal.
- The Manager web application is now deployed by the API Server. Installation is carried out using the **Server | Web | Business API Server | Manager** machine role.

  > **NOTE:** The previous Manager web application is no longer supported. Uninstall the Manager web application.

Target system connection

- Methods for authentication on the phone can be kept in Microsoft Entra ID user accounts.

  A patch with the patch ID ADO#430566 is available for synchronization projects.
- Microsoft Entra ID delta synchronization supports the "sync from now" feature.
- The Microsoft Entra ID connector now supports multi-value custom Microsoft Entra ID schema extensions.
- Windows Server 2025 support for Active Directory synchronization. Support for delegated managed service accounts (dMSA).

  A patch with the patch ID ADO#449910 is available for synchronization projects.
- Support for Microsoft Exchange Server Subscription Edition (Exchange Server SE).
- Windows Server 2025 support for Active Roles synchronization.

  A patch with the patch ID ADO#449910ARS is available for synchronization projects.
- For LDAP synchronization projects, you can specify how to perform the certificate revocation check.
- Personal ID data from SAP HCM systems (infotype 185) can be synchronized and provisioned.

  A patch with the patch ID ADO#388969 is available for synchronization projects.
- Allows synchronization of cost centers, operating codes, and cost codes from SAP HCM

systems. The **SAP HCM employees and departments** project template has been expanded to include corresponding synchronization steps and mappings. SAP HCM job descriptions on business roles can also be mapped in One Identity Manager.

A patch with the patch ID ADO#487238 is available for synchronization projects.

- Support for SMTP forwarding addresses for Exchange Online mailboxes.

  A patch with the patch ID ADO#458274 is available for synchronization projects.

- The `SendAs` and `FullAccess` permissions for Exchange Online mail users can be synchronized.

  A patch with the patch ID ADO#461817 is available for synchronization projects.

Identity and Access Governance

- As part of Behavior Driven Governance, One Identity Manager provides various company and attestation policies to test and recertify or remove access to SAP systems depending on usage patterns. On the one hand, this can reduce the risk of an identity having unnecessary authorizations or invalid authorization combinations. And on the other hand, it is possible to ensure that only authorizations that are actually required are included in the system measurement. This is done by analyzing the statistics on transaction usage per user account.
  - An ABAP function module for reading SAP usage data is provided that selects transaction calls per user and provides them as a list.
  - The SAP R/3 connector provides SAP usage data as separate schema types.
  - Features in the Manager for displaying SAP user accounts, SAP profiles, and SAP roles usage data.
  - There are default policies available for the following tasks:
    - Find SAP roles and profiles that were not used by anyone in a specified time period.
    - Find SAP user accounts with unused SAP roles or profiles.
  - New **TargetSystem | SAPR3 | BDG | UnusedThresholdInMonth** configuration parameter for approval recommendations based on the last SAP user account login.
  - New configuration parameter **TargetSystem | SAPR3 | BDG | DeleteDataOlderThan** and a new schedule **Clean up SAP usage data** to delete outdated SAP usage data.
- As part of Behavior Driven Governance, various company and attestation policies are provided to analyze Microsoft Entra ID applications usage and identify risky logins. This determines which users have access to which applications. Access can be recertified or removed.
  - The Microsoft Entra ID connector synchronizes application usage data and sign-in logs.

    > **NOTE:** A Microsoft Entra ID P1 license or P2 license is required to synchronize

> the sign-in logs.

  - Various reports are made available for evaluation.
  - New **TargetSystem | AzureAD | UnusedThresholdInMonth** configuration parameter for approval recommendations based on the last Microsoft Entra ID user account login.
  - A schedule is provided for clearing sign-in logs.

- One Identity Manager processes risk indexes from external applications and assigns them internally to identities. They are mapped as external risk indexes. They are included in the risk index calculation for identities in the same way as the internally recorded or calculated risk indexes.
  - New API project: `riskscore`
  - New calculation rule: **External risk index**
  - New schedule: **Updating and cleaning up external risk indexes**
- One Identity Manager supports identity threat detection and response (ITDR). If a threat is detected in an external system, a set of actions can be performed via a REST API call in One Identity Manager to minimize the effects of the threat. For example, affected identities can be deactivated, their user accounts blocked, and stakeholders informed. For this set of actions, ITDR playbooks are defined and default actions provisioned in One Identity Manager.

  Use the `secrets.json` configuration file to specify the database connection and authentication to use for the REST API call.
  - New API endpoints: `/ITDR/ListPlaybooks`, `/ITDR/RunPlaybook`, `/ITDR/InsertIncident`
- The default **Identity deputization** workflow is now used for delegation. This means that delegations created by the delegating identity or its manager are automatically approved. Delegations created by other identities require approval by the delegating identity or its manager. There is no longer a default compliance check.

  If delegations are to be approved by other approvers, change the assignment of the **Identity deputization** default approval policy to the **Deputy (temporary)** and **Delegation** service items.
- Certification status can be set manually or by attestation for system roles. The creation of new system roles can be configured so that they are automatically attested and certified.
  - New configuration parameters: **QER | Attestation | ESetApproval** and **QER | Attestation | ESetApproval | InitialApprovalState**
  - New attestation policy: **New system role certification**
  - New approval workflow: **New system role certification**
- New application role for synchronization project owners. This application role allows role-based login on the Synchronization Editor and the Operations Support Web Portal. Users with this application role:

    - Configure synchronization.
    - Edit synchronization templates.
    - Authorize other identities as owners.

  Saving a new synchronization project automatically creates a new application role for the synchronization project owners under the **Custom | Synchronization** application role. The identity that created the synchronization project and the target system managers automatically become members of this application role.

- In the Application Governance Module, applications can now be categorized by application type. The default delivery already contains the types:
    - Business application
    - Robotic process automation
    - Non-human process application

  Further types can be defined to suit customer requirements.

- The peer group factor is set to **-3** when inserting. This value indicates that the peer group factor was not calculated yet. As long as there is no peer group calculation in the workflow, an approver will no longer be shown any peer group-based recommendations.

Related topics

Enhancements

The following is a list of enhancements implemented in One Identity Manager 10.0.

Table 1: General

Enhancement	Issue ID
Improved support for translating lists with permitted values.	430677, 36702
Parameters set and their parameters can now be tested in the System Debugger.	430728
In the One Identity Manager History Database, the system configuration overview can now be queried via the `QBMVSystemOverview` view.	432014
In the Manager, the representation in the process information view of object data changes now shows the complete historical data from the entire recorded history, including the information from History Database.	463968
Machine roles for web servers can no longer be installed in the same folder	465029

Enhancement	Issue ID
as machine roles for workstations or servers.	
Improved performance running maintenance tasks for the database.	468867
The severity level of the **Tables deactivated by preprocessor with customer content** consistency check was changed to **Warning**.	472136
Transaction control in the `QBM_PColumnCustomRemove` procedure has been modified. Improved error messaging.	475077
Improved labeling and display of the `DialogTable.CacheInfo` property in the Designer.	477564, 471973
The script assembly for table scripts was renamed.	480411
Fallback support for SHA1 password hashing has been removed. This affects the authentication of users migrating from versions prior to One Identity Manager 7.0.	482752
Using the `AppServer.Installer.CMD.exe` command line program, History Database connection strings in `appsettings.json` can now be encrypted after installing the application server.	483197
Secure use of comparison operators (`<`, `>`, `<=`, `>=`) in query expressions is now permitted with appropriate permissions filtering.	483262
Support for optional parameters when calling methods via application servers.	488230
In the Manager, objects from other tables can now be assigned to several objects at the same time.	490265
Display values now support the multi-step resolution of foreign keys to display meaningful names instead of UIDs.	494280
Improved check in the application server front-end to determine whether automatic software updates are enabled.	496172
The `SendRichMail` process task of the `MailComponent` process component now allows emails to be sent without specifying the `Address` parameter, provided that either the `CC` or the `BCC` parameter is specified.	501914
The **No logging** and **Log changes**/**Log changes when deleting** properties can no longer be enabled at the same time.	507854

Enhancement	Issue ID
When checking additional view definitions (`QBMViewAddOn`) in the Designer, the column names in the SQL query are now also checked for validity.	508237
The Configuration Wizard now supports creation of new databases in Amazon RDS for SQL Server.	514236
OpenID Connect authentication now also uses claims from the ID token when a user info endpoint is configured to avoid issues with missing claims in Microsoft Entra ID.	541555
Improved support for SQL Server AlwaysOn availability groups, in particular Contained Availability Groups. **NOTE:** If the granular permissions concept is in use and the end user (`<DatabaseName>_User`) is to be used, then the permissions for `VIEW SERVER PERFORMANCE STATE` must be assigned manually. To do this, run the following SQL statement in a suitable program for running SQL queries. `grant VIEW SERVER PERFORMANCE STATE to <DatabaseName>_User`	546759

Table 2: API configuration

Enhancement	Issue ID
Adding new configuration keys has been reworked in the Administration Portal.	412459
If errors occur when validating a request made to the API Server, these are now output in the usual JSON format for error messages.	420303
When an API request with an Authorization header is processed, it is forwarded to the first available OAuth/OpenID Connect authentication module. The **QBM | AppServer | AccessTokenAuth** configuration parameter is no longer used.	420525
If there is no identity provider configured for a web application, the authentication modules for OAuth/OpenID Connect are not offered for selection on the corresponding login page.	427934
The API Server now emits the `Referrer-Policy: strict-origin-when-cross-origin` HTTP header by default.	450340

Enhancement	Issue ID
In the Administration Portal, the **Hide password properties in API responses (EnablePasswordApiProtection)** configuration key can now be used to specify whether password properties are hidden in API responses, even if the user has read permissions.	468665
The Administration Portal overview page has been reworked.	471029
In the Administration Portal, you can now configure API providers by creating a corresponding new configuration key.	479904
When you enable a disabled web application, you no longer need to restart the server.	480385
In the Administration Portal, the name of the **VI_ITShop_EnablePWOPriorityChange** configuration key has been clarified.	481014
The default application for the API Server is now **qer-app-portal**.	481965
In the Administration Portal, it is now possible to specify the validity of passcodes using the **Passcode validity (in hours) (VI_Employee_MasterData_PassCode_HoursValid)** configuration key.	507938

Table 3: HTML5 web development

Enhancement	Issue ID
Improved CDR support for properties of type **Bitmask**.	468856
Improved processing of date values with the **EndTime** configuration. You can now specify a time that is set by default to the end of the selected day.	473011
The web applications were updated to Angular 20.	503209
Improved security for queries using the **imx-version** header.	507519
The **imx/system** API endpoint only provides limited information about the system. To query the information previously provided under the **imx/system** API endpoint, use the **admin/systeminfo** API endpoint.	507520

Table 4: HTML5 web applications

Enhancement	Issue ID
Improved stability of web applications when indexing objects that are	232874

Enhancement	Issue ID
linked to a change label.	
When approving requests with rule violations in the Web Portal, exception approvers can now specify a date until which the exception remains valid. This date is used as the exception validity date and is independent of the request validity date.	407599
Improved error display for web applications when authenticating via an external identity provider.	417926
Statistics for the One Identity Manager History Database have been introduced into the Web Portal.	430245
There are new statistics available in the Web Portal.	430499, 471742
The web application login pages have been redesigned.	445134
In the Web Portal, on the **New request** page for service categories with child categories, the **Show products from child categories** option is now enabled by default.	459496
A new page with statistics has been added to the Operations Support Web Portal.	467642
Improved the **New Request** page in the Web Portal, which now supports filters and display settings.	467708, 463121
In the Operations Support Web Portal, you can now display a license report under **System > License Report**.	469351
Improved search on the **Responsibilities of My Reports** page in the Web Portal. You can now search for identity names and the names of the objects they are responsible for.	469667
In the Web Portal, the **Responsibilities of My Reports** page now supports view settings.	469668
In the Web Portal, additional filter options have been added for attestations.	470435
Improved the progress indicator on the **Attestation Runs** page in the Web Portal.	470994

Enhancement	Issue ID
Improved how the Web Portal displays charts for applications.	471024
Improved how the Web Portal displays the request renewal date in the request history	475652
In the Web Portal, some tiles on the start page have been renamed.	478012
Creating reports in the Web Portal is now linked to the **Portal_UI_CreateReports** program function. Only users who are assigned this program function can create new reports.	487105
In the Web Portal, SAP roles are now analyzed in the loss of entitlements due to attestations analysis.	490209
Improved and reworked how the process history is displayed in the Operations Support Web Portal.	496047
The **Process steps per process** page was removed from the Operations Support Web Portal.	496705
Improved and reworked the main object search in the Operations Support Web Portal. The search is now located in the Operations Support Web Portal header bar.	497212
In the Web Portal, it is now possible to find a policy violation using the name of the violating object.	497575
Improved and reworked how processes are displayed in the Operations Support Web Portal.	500015, 493660, 493659, 470991, 469872
In the Operations Support Web Portal, the **Web Applications** page has been moved to **Configuration > Basic Data > Security settings > Web applications**.	505848
In the Web Portal, the view for an approver of a request with multiple rule violations has been reworked.	506868
The database protocol was revised in the Operations Support Web Portal.	545562
The Operations Support Web Portal Job server overview has been reworked.	546757

Table 5: Target system connection

Enhancement	Issue ID
The active plan version for HR assignments in an SAP HCM system is loaded by the SAP connector using the **RH_INTERNAL_ACTIVE_WF_PLVAR** function and used automatically. If no other plan version is defined, the value **01** is assumed.	475884
Improved performance when synchronizing SAP authorizations.	448847
In the Synchronization Editor, you can set synchronization projects to open in read-only mode by default. This means that the open synchronization project is not locked for editing by other users. As soon as settings are changed, the current user has exclusive write access to the synchronization project.	487722
In the synchronization workflow, you can specify whether the general scope is taken into account when determining the revision information.	468570
Improved performance when displaying pending objects in the Manager. A maximum of 5000 objects are loaded initially. All other objects can be reloaded if required.	437383
If a SCIM provider does not provide a service provider endpoint, each endpoint contained in the resource type description is checked for acceptance of the `PATCH` verb when the schema is set up. If the test is successful, the result is saved to the schema type and the `PATCH` method is used for the update, otherwise `PUT`.	469641
Fractions of seconds were removed from the query used when loading object lists, as not all LDAP servers support this time format.	479960
The default setting for concurrency detection in startup configurations was changed from **Before processing** to **Before committing**. A patch with the patch ID ADO#509897 is available for synchronization projects.	509897
Attribute extensions for Microsoft Entra ID user accounts can be entered in One Identity Manager and provisioned in the target system under certain conditions. A patch with the patch ID ADO#474147 is available for synchronization projects.	474147
You can now select the authentication method when setting up Microsoft Exchange synchronization. A patch with the patch ID ADO#536601 is available for synchronization projects.	505661

Enhancement	Issue ID
You can now set the value of the API request in the connection configuration when setting up OneLogin synchronization. A patch with the patch ID ADO#542938 is available for synchronization projects.	542938
Risk index calculation rules and dependencies can now be defined in the Manager for custom model extensions to calculate risk indexes for default tables or custom tables (`RiskIndexCalculated`, `RiskIndexReduced`, `CCC_RiskIndexCalculated`, `CCC_RiskIndexReduced`).	474286
If a cloud application for group memberships does not provide any information about the member type, the type can be determined from the `$ref` property if the object URL is entered there.	509312
New message if a remote connection for which the **ADGroupAuthentication** authentication method is configured with the value **IntegratedWindowsAuthentication** cannot be established when setting up synchronization.	510136
Improved logging when establishing a connection to the HCL Domino server. In addition, the Domino Availability Index is not checked for the value **0** anymore.	519094
Until now, depending on the user type, it was not possible to edit and provision various properties of SAP user accounts. A script for editability can now be entered in these columns.	545580
Deployment of the One Identity Manager SAP add-on allows reinstallation within the same release without a prior uninstall.	511992
Retries for HTTP requests can now be configured for Microsoft Entra ID synchronizations to counteract possible data replication delays in Microsoft Entra ID.	499065
Improved loading behavior of objects for Exchange Online single object synchronization.	470335
Additional information is displayed in the Synchronization Editor script library.	480467
The composition of the URL used for authentication has been changed for connections via the SCIM connector. • For a relative URI, the configured server URL including port is now	496622

Enhancement	Issue ID
placed in front of it. There is no longer a configured service endpoint as part of the URL for authentication. - Nothing changes if complete URLs are specified as the authentication endpoint or for configurations without a service endpoint. Incorrectly configured URLs are marked in the SCIM connection wizard. If a certificate-based login is being configured, the URL specifications in the configuration are checked for use of HTTPS. **NOTE:** For existing installations: Check your configured SCIM connections and modify them if necessary.	

Table 6: Identity and Access Governance

Enhancement	Issue ID
When saving an attestation procedure, the system now checks whether the dollar ($) notation in the **Related object 1-3 (template)** fields (`ObjectKey1` to `ObjectKey3` columns) ends with an `ObjectKey` column. The system checks whether $ notation is permitted with the attestation base object in the **Property 1-4 (template)** fields (`PropertyInfoPattern1` to `PropertyInfoPattern4` columns) and the **Grouping column 1-3 (template)** fields (`StructureDisplayPattern1` to `StructureDisplayPattern3` columns).	436527
When approving requests with rule violations in the Web Portal, exception approvers can now specify a date until which the exception remains valid. This date is used as the exception validity date and is independent of the request validity date. If the date expires, the next scheduled rule check determines whether there is a rule violation for the compliance rule in question.	446530
Adaptive cards for request procedures are now deleted immediately once the request has been approved in the Web Portal.	457030
In the Manager, when attestation policies are copied, the assigned attestation conditions (`AttestationWizardParm`) can optionally be copied.	457489
When compliance checking requests in the Web Portal, system roles that match SAP functions are also taken into account.	469181
The `CreateITShopOrder` method can now be used to create requests from	486314

Enhancement	Issue ID
direct assignments to system roles (`ESetHasEntitlement`).	
Improved performance of the `QER-K-ShoppingRackMemberDel` DBQueue Processor task (**Delete customer in the IT Shop**).	508257

Related topics

Resolved issues

The following is a list of issues that have been resolved in this version.

Table 7: General

Resolved issue	Issue ID
An error may occur in the wizard for creating an OAuth 2.0/OpenID Connect configuration if an application is already marked as the default.	388883, 36037
An error may occur when compiling scripts for the first time.	466291
The automatic software update disabled logging in containers.	471800
The `QBMCustomSQL` table may not contain any custom SQL functions if these were created outside of One Identity Manager.	472007
An error may occur when the Job Queue Info displays data from the process archive. Error message: `Object reference not set to an instance of an object.`	472468
Importing a transport with approval steps fails if the process steps are not clearly numbered.	475097
An error occurs when the Manager saves deferred operations. Error message: `[810303] Deferred operations: The combination of the fields Object key, Time to run must be unique.`	475808
Inconsistent behavior of deferred deletion settings (`DeleteDelayDays` and `DeleteDelayScript`) for M:N tables.	478580
The Database Agent Service attempts to run incorrectly configured, custom	481896

Resolved issue	Issue ID
DBQueue Processor tasks instead of logging a corresponding message.	
In the Object Browser, an error occurs when editing objects using multi-select when a connection is established via the application server.	485653
The Manager no longer displays conflict handling for simultaneous changes by other users.	487130
Updating an installation may not trigger an automatic software update, resulting in updated and custom files being missing from the installation folders.	487806
An empty `IN` clause results in invalid query syntax and parsing errors in the application server.	488812
Performance issue when optimizing `WHERE` clauses for permissions groups.	488841
Under certain conditions, role-based login to the application server results in an endless loop while loading.	489421
An error occurs loading external components in the `ScriptComponent` process component.	496366
Using an import script to import data may result in an error. Error message: `The assembly 'System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' could not be found., at VI.Base.AssemblyLoader._LoadFrom(AssemblyName asmName, Boolean throwOnException)`	496466
The `AppServer.Installer.CMD.exe` command line program writes the connection information for an additional History Database connection to the `Web.config` file instead of the `appsettings.json` file.	496694
The System Debugger fails to save the contents of a new script in the database.	496794
Canceling the One Identity Manager uninstall dialog started from "Apps and Features" in the Control Panel, still completely deletes the application.	497576
In the Manager, running tasks on a multi-select object does not work from the context menu.	498824
Deactivating authentication modules for the Manager application has no	498862

Resolved issue	Issue ID
effect.	
When the Object Browser applies templates to multiple selected objects, only the first object is updated if the connection was established via the application server.	498931
The SQL Formatter adds a `LEFT(<column>, 512)` function in `ORDER BY` clauses. This prevents database indexes from being used and slows query performance when loading paginated collections.	498952
Historical assignments in reports display the wrong user when an assignment is created.	499206
Event names for processes that differ only in special characters (such as spaces or hyphens) lead to errors during compilation.	501706
A script for deferred deletion, which calculates the deletion time based on a to the minute or an hourly-based time period, incorrectly sets the deletion time to the current time. This causes the delayed operation to be performed immediately.	501808
Bearer authentication does not work with Microsoft Entra ID because the UserInfo endpoint does not provide the ID token or the required claims.	502606
Missing permissions for end users to perform delegations.	505164
Processing information is removed from the database even though IT Shop requests for the GenProcID are still being processed.	505838
If there are deferred tasks in the DBQueue, the Database Compiler waits a long time for the DBQueue Processor before compilation is possible.	506979
Under certain conditions, the Database Agent Service is terminated too quickly during migration.	509905
Performance issue generating an `SQL COUNT` query with permissions filters that are concatenated by `OR` clauses.	512854
The automatic software update causes problems with the naming of start menu entries and services.	513935
In the object properties dialog, it is no longer possible to switch between the simple and the expanded view of the columns.	519063

Resolved issue	**Issue ID**
Using role-based logins, an error occurs when displaying historical data in TimeTrace. Error message: `Document (...) could not be opened! Missing value XUpdateMask.`	528847
The Schema Extension hides the **Save to file** option for saving schema changes.	530686
An error occurs when opening statistics containing a tachometer chart. Error message: `Document (...) could not be opened! Sequence contains no elements.`	542386
Single-user mode is still required too often for importing transports.	545730
During installation of the application server using the Web Installer, permissions for the private key file cannot be set for the session certificate that was created. This causes an HTTP 500 error in the application server. Error message: `Error trying to resolve Service 'QBM.AppServer.Base.ISessionStore' or one of its autowired dependencies (see inner exception for details).`	635863
The Manager may display the filter dialog for restricting list entries even though no query limit has been set.	645823
Performance issues loading result lists when the Manager displays additional columns.	646042

Table 8: API configuration

Resolved issue	**Issue ID**
Under certain conditions, processing interrupted HTTP requests made to the API Server results in an error on the SQL Server.	500623

Table 9: HTML5 web applications

Resolved issue	**Issue ID**
In the Web Portal, the name or description of an attestation case on the **Pending Attestations** page does not mention the name of the corresponding system entitlement.	459200
In the Web Portal, it is not possible to change the displayed selected items on the **New Request** page.	463114

Resolved issue	Issue ID
It is not possible to select certain responsibilities on the **Responsibilities of My Reports** page in the Web Portal.	468193
In the Web Portal, reassignment of a responsibility can cause an error.	468349
Web applications do not always regenerate the CAPTCHA code after a failed login.	472460
The email link for replying to a request inquiry in the Web Portal does not work.	483102
The link in an email regarding the approval decision about a request in the Web Portal does not work.	493153
Under certain conditions, the Web Portal does not display a message if an error occurs in a custom validation script.	496025
The units for values in the statistics are missing in the Web Portal.	497103
Under certain conditions, a link on the **Policy Violations** page in the Web Portal does not point to the correct display.	497218
Under certain conditions, sending request inquiries in the Web Portal results in an error.	498871
Under certain conditions, the Web Portal does not display the hyperview of the violating object for a policy violation.	499229
The Web Portal has an issue when the valid-from date is set in Slovenian format during delegation.	502448
The Web Portal allows identities to be created on the start page in the **My Direct Reports** tile even though creating identities is disabled.	502483
The Web Portal only displays the loss of entitlements analysis for one attestation case, even though several are selected.	502805
Some application KPIs deliver incorrect results in the Web Portal.	542175
Under certain circumstances, an error occurs in the Web Portal when requesting memberships for a system role.	645503

Table 10: Target system connection

Resolved issue	Issue ID
Provisioning requests fail if encrypted values contain certain special characters.	460942
Error creating a new synchronization project from a configuration file (`*.sews`) with the Synchronization Editor Command Line Interface. Error message: `Object of type 'System.String' cannot be converted to type 'System.Security.Principal.IPrincipal'.`	468086
There is an issue using multi-line variable values in synchronization projects. A patch with the patch ID ADO#471688 is available for synchronization projects.	471688
The wizard for creating a new base object in the Synchronization Editor cannot create a target system connection. Error message: `Value cannot be null. (Parameter 'iocContainer')`	477522
An error occurs in the Exchange Online connection wizard when saving custom connector definitions.	480412
Performance problems and errors when synchronizing SharePoint Online site collections with **NoAccess** status.	488015
An error occurs in the Synchronization Editor if the RemoteConnectPlugin with the **SecretAuthentication** authentication method is configured for One Identity Manager Service. Error message: `Response status code does not indicate success: 401 (Unauthorized).`	492982
The SCIM provider interprets Base64-encoded IDs incorrectly.	495673
Error (`System.NullReferenceException`) when synchronizing an external database via the generic ADO.NET provider.	496240
If the last member is removed from a group in One Identity Manager and the change is provisioned in the cloud application, this group membership is not deleted in the cloud application.	500950
It is possible to delete an Active Directory container, even if the **Protected from accidental deletion** option is enabled for the object.	502583
If the reload threshold is set very high in a synchronization project and the object list contains complex attributes, the SCIM connector does not access	503026

Resolved issue	Issue ID
all subattributes individually.	
When testing the settings for connecting to a central system of a CUA, a warning is always displayed.	507489
There is an issue running the `SAP_Person_Update_CommunicationData` process if the identity has multiple SAP user accounts with the **Full managed** automation level.	509011
Synchronization does not ignore memberships that still have pending processes in the Job queue.	509891
Syntax error provisioning deleted `CSData` attributes in IBM RACF.	532114, 645587
If an insert operation using the RACF LDAP connector fails, no error is displayed in the synchronization log.	532114, 646094
The audit logs for One Identity Safeguard only show entries for one day.	542496
Saving modified synchronization projects (containing a UTF-8 BOM) in the database causes an error if the connection is established via the application server. Error message: `[810092] <name and display of sync project> was changed by another user. VI.Base.ViException: Error applying changes to database.`	542688
An error occurs during synchronization if a schema property name contains two dollar signs and it is used in scripts.	544410
The Synchronization Editor does not display the configuration variables for the OneLogin connector connection timeout and OAuth authorization type.	546063
The connection to an SAP schema extension file and to the CUA central system cannot be established if a remote connection is used for connecting to the SAP R/3 system.	646079

Table 11: Identity and Access Governance

Resolved issue	Issue ID
Error approving an exception for a rule violation by a deputy of the exception approver. Error message:	474928

Resolved issue	Issue ID
`The identity cannot grant an exception for this rule violation.`	
Error assigning sampling items to a sample for attestation. Error message: `Document (<name>) could not be opened! Sequence contains no matching element.`	481992
Not approved before (`AttestationCase.IsNotApprovedBefore`) is not set correctly for attestation cases that are created by a scheduled task.	483355
When compliance checking requests, the OH approval procedure not only determines the exception approvers of the compliance rule posing the highest threat, but also the exception approvers of all violated rules. In addition, in some cases, an incorrect value is set for `PWOHelperPWO.Decision`, so that no approval decision can be made.	487239
There is an issue moving multiple products to another IT Shop shelf. Error message: `Database error 2627: Violation of PRIMARY KEY constraint 'PK__#Struktu__65E8195C95BFC29A'. Cannot insert duplicate key in object 'dbo.#Structure'.`	496360
There is an issue creating software applications. Error message: `Value IsProfileApplication was not found.`	502801
The email used to notify attestors when approvals are delegated contains incorrect links for locating the attestation case.	508126
Various problems with the `ATT_PAttestationHelperFill` procedure in connection with deputization.	508773
The **System halt (days)** setting in approval workflows has no effect if there are still long-running processes in the Job queue for this approval process.	508927
It is not possible to create a deputy if one already exists for the same period and recipient with **Canceled** status.	518248
The **Approval of Microsoft Entra ID requests** approval workflow stays in an endless loop if the target system manager does not define an owner for the requested authorization object.	518810
Error running the `VI_ITShop_Process Approval Inbox` process. Error message:	541656

Resolved issue	Issue ID
`[Microsoft.Exchange.WebServices.Data.ServiceRequestException] The request failed. The remote server returned an error: (401) Unauthorized.`	
Error copying an attestation case which has a report assigned to it. Error message: `PWODecisionStep: Write permission denied for value "CountApprover".`	544132
Inaccurate display of request properties with multi-value request parameters.	545501
The `FillOrder` method can be used to create request for identities that are not allowed to request the product.	580738

Related topics

Known issues

The following is a list of issues known to exist at the time of release of this version.

Table 12: General

Known Issue	Issue ID
Error in the Report Editor if columns are used that are defined as keywords in the Report Editor. Workaround: Create the data query as an SQL query and use aliases for the affected columns.	23521
Access errors can occur if several instances of the Web Installer are started at the same time.	24198
Headers in reports saved as CSV do not contain corresponding names.	24657
Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation. Cause: The Configuration Wizard was started directly. Solution: Always use `autorun.exe` for installing One Identity Manager components. This ensures that you do not select any invalid modules.	25315
Error connecting via an application server if the certificate's private key,	27793

Known Issue	Issue ID
used by the `VI.DB` to try and encrypt its session data, cannot be exported and the private key is therefore not available to the `VI.DB`. Solution: Mark the private key as exportable if exporting or importing the certificate.	
Error resolving events on a view that does not have a UID column as a primary key. Primary keys for objects in One Identity Manager always consist of one, or in the case of M:N tables, two UID columns. This is basic functionality in the system. The definition of a view that uses the `XObjectKey` as primary key, is not permitted and would result in more errors in a lot of other places. The consistency check **Table of type U or R with wrong PK definition** is provided for testing the schema.	29535
If the One Identity Manager database is installed in an SQL cluster (High Availability Group) and the option `DTC_SUPPORT = PER_DB` is set, replication between servers is done by Distributed Transaction. If a `Save Transaction` is run in the process, an error occurs: `Cannot use SAVE TRANSACTION within a distributed transaction.` Solution: Disable the option `DTC_SUPPORT = PER_DB`.	30972
If no date is given, the date 12/30/1899 is used internally. Take this into account when values are compared, for example, when used in reports. For more information on the use of dates, see Notes on using date values.	31322
Variables are used in a report and there are customized translations given for these variables in the Report Editor. However, the variables are not translated in the report that is generated. Cause: When reports are generated, the translations of default variables as displayed in the Report Designer dictionary below the **Quest** category are overwritten with the values from the One Identity Manager database. Solution: Create your own variables and store them outside of the **Quest** category in the Report Designer dictionary. These variables can be translated.	36686
The consistency check **Columns of type varchar(38) not PK and not FK.** identifies issues with columns that are `varchar(38)` long but are not labeled as UID columns. Solution: Choose a different column length when extending the schema. According to the modeling guidelines, columns with a length of `varchar(38)` are reserved for columns that map a UID.	37072
Installing web applications using the Web Installer in a virtual machine (VM) is not supported if the installation source is located in a shared folder such as a local folder on the VM host that is provided to the VM as a new file	471381

Known Issue	Issue ID
drive. The event log may display error messages for **Source = Application error** and **Incorrect application name: WebInstaller.exe**. Workaround: Use a network share and assign it to a free drive letter in your VM.	

Table 13: HTML5 web applications

Known Issue	Issue ID
The error message `This access control list is not in canonical form and therefore cannot be modified` sometimes occurs when installing the Web Portal with the Web Installer. The error occurs frequently after a Windows 10 Anniversary Update. Solution: Change the permissions for the users on the web application's parent folder (by default `C:\inetpub\wwwroot`) and apply the changes. Then revoke the changes again.	26739
In the Web Portal, a product's request properties are not transferred from the original request to the shopping cart if the request is renewed or canceled. Cause: Request properties are saved in separate custom columns. Solution: Create a template for (custom) columns in the `ShoppingCartItem` table that stores the request properties when the request is made. This template must load the request properties from the identical (custom) columns in the `PersonWantsOrg` table relating to this request.	32364
In the Web Portal search, if you enter a search term and then group the data, the view also displays empty groups.	468982

Table 14: Target system connection

Known Issue	Issue ID
Memory leaks occur with PowerShell connections, which use `Import-PSSession` internally.	23795
By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely. Solution: Make it possible to access the building block **HR_ENTRY_DATE** remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate` in the Synchronization Editor.	25401
Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no	27042

Known Issue	Issue ID
primary SIP addresses are stored until now.	
Error in Domino connector (`Error getting revision of schema type ((Server))`). Probable cause: The HCL Domino environment was rebuilt, or numerous entries have been made in the Domino Directory. Solution: Update the Domino Directory indexes manually in the HCL Domino environment.	27126
The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3. If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration. • Add a custom column to the table `SAPUser`. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required.	27359
Error provisioning licenses in a central user administration's child system. Message: `No company is assigned`. Cause: No company name could be found for the user account. Solution: Ensure that either: • A company, which exists in the central system, is assigned to every user account. - OR - • A company is assigned to the central system.	29253
Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will come into effect later. Cause: The `BAPI_EMPLOYEE_GETDATA` function is always run with the current date. Therefore, changes are taken into account on the exact day. Solution: To synchronize personnel data in advance that comes into effect later, use a schema extension and load the data from the table `PA0001` directly.	29556
Target system synchronization does not show any information in the Manager web application. Workaround: Use Manager to run the target system synchronization.	30271
Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping	31017

Known Issue	Issue ID
is disabled. Cause: The SharePoint connector loads all object properties into cache by default. Solution: • Correct the error in the target system. - OR - • Disable the cache in the file `VI.Projector.SharePoint.<Version>.Host.exe.config`.	
If a SharePoint site collection only has read access, the server farm account cannot read the schema properties `Owner`, `SecondaryContact`, and `UserCodeEnabled`. Workaround: The properties `UID_SPSUserOwner` and `UID_SPSUserOwnerSecondary` are given empty values in the One Identity Manager database. This way, no load error is written to the synchronization log.	31904
If date fields in an SAP R/3 environment contain values that are not in a valid date or time formats, the SAP connector cannot read these values because type conversion fails. Solution: Clean up the data. Workaround: Type conversion can be disabled. For this, SAP Connector for Microsoft .NET for .NET 4.0 on x64, version 3.0.15.0 or later must be installed on the synchronization server. **IMPORTANT:** The solution should only be used if there is no alternative because the workaround skips date and time validation entirely. ***To disable type conversion*** • In the `StdioProcessor.exe.config` file, add the following settings. • In the existing `<configSections>`:	32149

```
<sectionGroup name="SAP.Middleware.Connector">

<section name="GeneralSettings" type="SAP.Middleware.C
onnector.RfcGeneralConfiguration, sapnco, Versio
n=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c
7f7d23" />

 </sectionGroup>
```

  - In the new section:

```
<SAP.Middleware.Connector>
```

Known Issue	Issue ID

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

The Google Workspace connector cannot successfully transfer Google applications user data to another Google Workspace user account before the initial user account is deleted. The transfer fails because of the Rocket application's user data. Workaround: In the system connection's advance settings for Google Workspace, save a user data transfer XML. In this XML document, limit the list to the user data to be transferred. Only run the Google applications that have user data you still need. For more information and an example XML, see Advanced settings for the system connection to Google Workspace.	33104
If target system data contains appended spaces, they go missing during synchronization in One Identity Manager. Every subsequent synchronization identifies the data changes and repeatedly writes the affected values or adds new objects if this property is part of the object matching rule. Solution: Avoid appending spaces in the target system.	33448
In the schema type definition of a schema extension file for the SAP R/3 schema, if a `DisplayPattern` is defined that has another name in the SAP R/3 schema as in the One Identity Manager schema, performance issue may occur. Solution: Leave the `DisplayPattern` empty in the schema type definition. Then the object's distinguished name is used automatically.	33812
After an update from SAP_BASIS 7.40 SP 0023 to SP 0026 or SAP_BASIS 7.50 SP 0019 to SP 0022, the SAP R/3 connector can no longer connect to the target system.	34650
After upgrading from One Identity Manager version 8.0 or version 8.1 to One Identity Manager version 8.2.1 or later, PowerShell scripts that reference the Az PowerShell module (`Import-Module Az`) may not work. In a PowerShell launched on the same host, the scripts work without errors. Error messages are logged when the `ExecuteScript` process task is run by the `PowerShellComponentNet4` process component. Example: `Entry point was not found.` Cause: One Identity Manager version 8.2.1 or later, ships with a specific version of an `Azure.Core.dll` library. The custom PowerShell script may however	430202, 37116

Known Issue	Issue ID

depend on a newer version of the Az PowerShell module. When the One Identity Manager Service runs the script, it uses the locally stored `Azure.Core.dll`, breaking the dependency.
Possible workarounds: Check whether the following workarounds might work with respect to input parameter and return value.
• Call PowerShell as a subprocess
To run a PowerShell command out of the current process, start a new PowerShell process directly with the command call:
`pwsh -c 'Invoke-ConflictingCommand'`
• Use the `CommandComponent` process component with the `Execute` process task to launch the PowerShell application with the following command call.
`powershell -c 'Invoke-ConflictingCommand'`	

The following error occurs in One Identity Safeguard if you request access to an asset from the access request policy section and it is configured for asset-based session access of type **User Supplied**: `400: Bad Request -- 60639: A valid account must be identified in the request.` The request is denied in One Identity Manager and the error in the request is displayed as the reason.	796028, 30963
After updating to One Identity Manager version 9.3 or later, scripts in synchronization projects that use custom DLLs can no longer be translated. Cause: Conversion of One Identity Manager base technology. Solution: 1. Transfer these scripts to the Synchronization Editor script library as external scripts. 2. Customize the script code for the use of NuGet packages. 3. Compile the scripts.	463957
The One Identity Safeguard connector connection to a One Identity Safeguard appliance quits with following errors: `System.Management.Automation.RuntimeException] (7,36): error SYSLIB0014: 'ServicePointManager' is obsolete: 'WebRequest, HttpWebRequest, ServicePoint, and WebClient are obsolete. Use HttpClient instead. Settings on ServicePointManager no longer affect SslStream or HttpClient.' (https://aka.ms/dotnet-warnings/SYSLIB0014)`	647286

Known Issue	Issue ID
`public static void SetCallback() { System.Net.ServicePointManager.ServerCertificateValidationCallback = ValidationCallback; }` Cause: The PowerShell cmdlets published with One Identity Safeguard 7.0 and 7.5 no longer work in .NET 10 runtime environments. Solution: Use One Identity Safeguard as from version 8.0. You will find a matching One Identity Manager module for each version supported on the PowerShell installation medium in the `Modules\PAG\dvd\AddOn\safeguard-ps` directory. Versions without a matching PowerShell module on the One Identity Manager installation medium, are not supported.	

Table 15: Identity and Access Governance

Known Issue	Issue ID
During approval of a request with self-service, the `Granted` event of the approval step is not triggered. In custom processes, you can use the `OrderGranted` event instead.	31997
If an assignment is inherited through a role hierarchy, **bit 1** is set on the inherited assignment. Inherited assignments are consequently always indirectly assigned, even if they were originally created directly by a dynamic role or an assignment request.	35193
If a service item has its **Max. days valid** option reduced such that approved requests are already expired, these requests cannot be unsubscribed anymore. Solution: Create a process for the `AccProduct` base object that is triggered when changes are made to `AccProduct.MaxValidDays`. The process calculates the 'valid until' date for these requests (`PersonWantsOrg.ValidUntil`) from `PersonWantsOrg.ValidFrom` and `AccProduct.MaxValidDays`. After which, you can unsubscribe the requests.	36349

Table 16: Third party contributions

Known Issue	Issue ID
Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting **File and Printer sharing** is not set on the server. This option is not set on domain controllers on the grounds of security.	24784
An error, TNS-12516, TNS-12519 or ORA-12520, sporadically occurs when connecting with an Oracle Database. Reconnecting normally solves this.	27830

Known Issue	Issue ID
Possible cause: The number of processes started has reached the limit configured on the server.	
Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages. Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.	29051
Memberships in Active Directory groups of type **Universal** in a subdomain are not removed from the target system if one of the following Windows updates is installed: • Windows Server 2016: KB4462928 • Windows Server 2012 R2: KB4462926, KB4462921 One Identity does not know whether other Windows updates also cause this error. The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory group provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem.	30575
Under certain conditions, the wrong language is used in the Stimulsoft controls in the Report Editor.	31155

In certain Active Directory/Microsoft Exchange topologies, the `Set-Mailbox` Cmdlet fails with the following error:
`Error on proxy command 'Set-Mailbox...'`
`The operation couldn't be performed because object '...' couldn't be found on '...'.`
For more information, see https://support.microsoft.com/en-us/help/4295103.
Possible workarounds:
• Connect to the Microsoft Exchange server that the user mailbox is on. Use a custom process to do this. Use the `OverrideVariables` parameter (`ProjectorComponent` process component) to overwrite the server (`CP_ExchangeServerFqdn` variable).
• Because this problem only occurs with a few schema properties, you should consider protecting these schema properties in the synchronization project against write operations. You can set the schema properties in a custom process using the `PowershellCompomentNet4` process component through a user-defined PowerShell call.
	33026

Schema changes

The following provides an overview of schema changes from version 9.3.1 up to version 10.0.

Configuration Module

- New tables `QBMCEFDefinition` and `QBMCEFMessage` for mapping SIEM messages.
- The `QBMCEFDefinitions` table was deleted. Existing data is transferred to the `QBMCEFDefinition` table.
- New tables `QBMAttribute` and `QBMAttributeAssign` for mapping additional database schema attributes.
- New table `QBMLoginAudit` for recording logins and logouts.
- New column `QBMDBQueueTask.BulkLimit` for setting an upper limit for bulk processing.
- New columns `DialogColumn.MinValue` and `DialogColumn.MaxValue` for specifying a minimum value and a maximum value.
- New columns `DialogColumn.UIInfo`, `DialogValidDynamicRef.UISlimCreationTemplate`, and `QBMRelation.UISlimCreationTemplate` for configuring the slim creation of referenced objects on main data forms.
- New column `DialogColumn.UIWidth` for the width of an input field on generic forms.
- New column `DialogDatabase.UID_SingleUserSession` in preparation for future features.
- New columns `DialogValidDynamicRef.UIGetFilterScript` and `QBMRelation.UIGetFilterScript` in preparation for future features.
- The `DialogUserDisplayConfig.Element` column was extended to `varchar(max)`.

Intelligent Query Chatbot Module

- New data model for the Intelligent Query Chatbot Module.

Target System Synchronization Module

- New `DPRLastModification` table for mapping change data that deviates from the configured revision filtering.
- New column `DPRProjectionConfig.TryGetRevisionUsingScopeFilter` to specify whether to take the general scope into account when determining revision data.
- New column `DPRRevisionStore.IsFiltered` to flag whether the revision was filtered.
- New column `DPRSystemVariable.IsMultiLine` for multiline content.

Microsoft Entra ID Module

- New table `AADSignIn` for mapping Microsoft Entra ID sign-in logs.
- New table `AADUserApplicationUsage` for mapping application usage.
- New table `AADUserPhoneAuthMethod` for mapping authentication methods on the phone.
- New columns `AADOrganization.RetainRiskSignIns`, `AADOrganization.RetainRiskSignInWhereClause`, `AADOrganization.RetainSignInEntriesForDays` and `AADOrganization.RetainSignInWhereClause` for mapping sign-in log data.

Exchange Online Module

- New table `O3EMailUserSendAsPerm` for mapping send permissions for Exchange Online.
- New column `O3EMailbox.ForwardingSmtpAddress` as SMTP forwarding address.

SAP R/3 User Management Module

- New column `SAPProfile.HasReadOnlyMemberships` to specify whether memberships are read-only.

SAP R/3 Structural Profiles Add-on Module

- New table `SHRPersonPersonalID` for mapping personal IDs from SAP HCM systems.

Domino Module

- The columns `NDOServer.FileName`, `NDOServer.Password` and `NDOUser.SecurityType` were deleted.

Identity Management Base Module

- New columns `PersonWantsOrg.ExceptionValidUntil` and `PWODecisionHistory.ExceptionValidUntil` that allow exception approvers to set a validity date for the exception approval when approving requests with rule violations.
- New table `QERExternalRiskScore` for mapping external risk index values.
- New columns `BaseTree.CanonicalName`, `BaseTree.DistinguishedName`, `BaseTree.InternalType` and `ProfitCenter.CanonicalName`, `ProfitCenter.DistinguishedName`, `ProfitCenter.InternalType` for mapping additional organizational data from SAP HCM systems.
- New table `QERVShellOwnerUsage` and new column `DPRShell.UID_AERoleShellOwner` as application role for synchronization project owners.

- New table `QERCloudAssistantMessage` for mapping Starling Cloud Assistant approval messages.

System Roles Module

- New column `ESet.ApprovalState` for certifying system roles.

Attestation Module

- New column `AttestationWizardParm.WhereClause` as a condition for selecting objects.

Company Policies Module

- New tables `POLPlaybook`, `POLPlaybookAction`, `POLPlaybookHasAction`, `POLPlaybookRun` for mapping ITDR playbooks.

SAP R/3 Compliance Add-on Module

- New tables `SAPUserUsesTransaction` and `SAPProfileHasTCD` for mapping SAP usage data.
- New table `SAPESetInSAPFunction` for system roles that match SAP functions.
- The `SAPVariableSetDetail.VariableValue` column has been extended to `nvarchar(max)`.

Application Governance Module

- New table `AOBApplicationType` and new columns `AOBApplication.UID_AOBApplicationType` and `AOBApplication.UID_PersonMachineIdentity` for mapping application types.

Changes to system connectors

The following provides an overview of the modified synchronization templates and an overview of all patches supplied by One Identity Manager version 9.3.1 up to version 10.0. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects.

New and deleted synchronization templates

The following provides an overview of new and deleted synchronization templates.

Patches are provided for changes to existing synchronization templates. For more information, see Patches for synchronization projects.

Table 17: Overview of synchronization templates

Module	Synchronization template	Type of modification
Microsoft Entra ID Module	Microsoft Entra ID audit	new
SAP R/3 Compliance Add-on Module	SAP usage data	new

Patches for synchronization projects

Patches for the following patch types are provided in One Identity Manager 10.0.

- Patches for resolved issues
- Patches for new features
- Milestones

To adjust existing synchronization projects to One Identity Manager version 10.0, you must implement milestones. A milestone is provided for each context. A milestone includes all patches for resolved issues together with milestones from previous versions, if they have not already been implemented. Once the current milestone has been implemented in a synchronization project, the project is then compatible with One Identity Manager 10.0.

Patches for new features can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 10.0 for synchronization projects. Only the patches that were newly created after version 9.3.1 are listed. For information about patches from earlier versions of One Identity Manager, see the respective release notes for each version.

Every patch contains a script, which tests whether the patch can be applied to the synchronization project. This depends on the specific configuration of the synchronization.

> **TIP:** Implement milestones first and then apply optional patches for new features.

For more information, see Applying patches to synchronization projects.

Table 18: General patches

Patch ID	Patch	Description	Issue ID
ADO#509897	Changes the default behavior of collision detection	Changes the default setting for collision detection in the startup configuration to **Before committing**.	509897

Table 19: Patches for Microsoft Entra ID

Patch ID	Patch	Description	Issue ID
ADO#474147	Enables provisioning of attribute extensions for Microsoft Entra ID user accounts	Updates the **User** mapping to enable provisioning of attribute extensions (`OnPremisesExtensionAttributes`). This patch is applied automatically when One Identity Manager is updated.	474147
ADO#430566	Support for synchronizing methods of authentication on the phone	New mapping and new workflow for synchronizing methods for authenticating users on the phone. This patch is applied automatically when One Identity Manager is updated.	430566

Table 20: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
ADO#449910	Support for delegated managed service accounts	Updates the **user** mapping so that delegated managed service accounts can be synchronized.	449910

Table 21: Patches for One Identity Active Roles

Patch ID	Patch	Description	Issue ID
ADO#449910ARS	Support for Windows Server 2025	Updates the schema property `vrtDomainFunctionalLevelString` in the **Domain** mapping to support Windows Server 2025. This patch is applied automatically when One Identity Manager is updated.	449910

Table 22: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
ADO#536601	Support for various authentication methods	Adds a new connection parameter for selecting the authentication method.	505661

Patch ID	Patch	Description	Issue ID
		This patch is applied automatically when One Identity Manager is updated.	

Table 23: Patches for Google Workspace

Patch ID	Patch	Description	Issue ID
ADO#471688	Support for multiline variables	Sets the **Multiline** property for the `CP_ServiceAccountJson` variable.	471688

Table 24: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
ADO#458274	Support for SMTP forwarding addresses	Inserts a property mapping rule for mapping SMTP forwarding addresses into the **Mailbox** mapping. This patch is applied automatically when One Identity Manager is updated.	458274
ADO#461817	Send permissions mapping for Exchange Online mail users	New mapping and new synchronization step **MailUser Permissions** for mapping send permissions for Exchange Online mail users. This patch is applied automatically when One Identity Manager is updated.	461817

Table 25: Patches for OneLogin

Patch ID	Patch	Description	Issue ID
ADO#542938	Support for connection timeout	Inserts a new connection parameter for a connection timeout. This patch is applied automatically when One Identity Manager is updated.	542938

Table 26: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
ADO#487238	Integration of additional HCM data	New mappings and synchronization steps for mapping cost centers, booking codes, cost codes, and job descriptions.	487238

Patch ID	Patch	Description	Issue ID
ADO#388969	Integration of personal ID data	New mapping and new synchronization step for mapping personal ID data (infotype 185).	388969

Deprecated features

The following features are no longer supported with this version of One Identity Manager:

- Windows Server 2012 and Windows Server 2012 R2 are no longer supported.
- The previous Manager web application is no longer supported. Uninstall the Manager web application. Use the Manager web application, which is deployed via API Server instead.
- Exchange Online via Exchange Web Services will no longer be supported for email notifications in the future. If you continue using an Exchange Online mailbox, we recommend using a Microsoft Graph-based connection with the Microsoft 365 mail system.
- The **QER | Attestation | MailApproval | Mailsystem | Exchange | AppId** and **QER | ITShop | MailApproval | Mailsystem | Exchange | AppId** configuration parameters have been deleted.
- Access to Azure access tokens now takes place in an isolated environment; the previous method is no longer supported.

  The following scripts were removed.

  - QER_GetAzureAccessTokenForUser
  - QER_GetAzureAccessTokenForApp
- The `QBM_ProcessOneCEFDefinition` script has been deleted.
- One Identity Safeguard versions 7.x are no longer supported.

The following features will be deprecated in future releases of One Identity Manager and should no longer be used:

- The process tasks `DelRoleFromUse`, `ADDINFOTYPE0105`, `UPDINFOTYPE0105`, and `DELINFOTYPE0105` from the `SAP Component` process components will be deprecated in future versions.
- The process tasks `AddMember` and `DelMember` from the `AD Component` process components will be deprecated in future versions.
- The scripts `VI_MassDelegate` and `VI_MassDeleteDelegate` as well as the processes `VI_ITShop_Person Mass Delegate` and `VI_ITShop_Person Mass End Delegate` will be deprecated in future versions.

System requirements

Before installing One Identity Manager 10.0, ensure that your system meets the following minimum hardware and software requirements.

For detailed information about system prerequisites, see Installation prerequisites.

> **NOTE:** When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. For more information about environment virtualization, see One Identity's Product Support Policies.

Every One Identity Manager installation can be virtualized. Ensure that performance and resources are available to the respective One Identity Manager component according to system requirements. Ideally, resource assignments for the database server are fixed. Virtualization of a One Identity Manager installation should only be attempted by experts with strong knowledge of virtualization techniques.

Supported database systems

One Identity Manager supports the following database systems:

- SQL Server
- Managed instances in the Azure SQL Database
- Azure SQL Database
- Amazon RDS for SQL Server

Minimum system requirements for implementing SQL Servers as database servers

A server must meet the following system requirements for installation of a One Identity Manager database. Depending on the number of One Identity Manager modules and the accounts managed in One Identity Manager, the requirements for working memory, hard disk storage, and processors may be significantly greater than the minimum requirements.

Table 27: Minimum system requirements for SQL Servers

Requirement	Detail
Processor	8 physical cores with 2.5 GHz+ frequency (non-production) 16 physical cores with 2.5 GHz+ frequency (production)

Requirement	Detail
	NOTE: 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM (non-production) 64 GB+ RAM (production)
Hard drive storage	100 GB
Operating system	Windows operating system • Note the requirements from Microsoft for the SQL Server version installed. UNIX and Linux operating systems • Note the minimum requirements given by the operating system manufacturer for SQL Server databases.
Software	Following versions are supported: • SQL Server 2022 Standard Edition (64-bit) with the latest cumulative update **NOTE:** For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems. **NOTE:** Ledger is not supported. For more information, see the Knowledge Base. • Compatibility level for databases: SQL Server 2022 (160) • Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) • SQL Server Management Studio (recommended)

> **NOTE:** The minimum requirements listed above are for general use. With each custom One Identity Manager deployment these values may need to be increased to provide ideal performance. To determine production hardware requirements, it is strongly recommended to consult a qualified One Identity Partner or the One Identity Professional

> Services team. Failure to do so may result in poor database performance.
>
> For additional hardware recommendations, read the KB article https://support.oneidentity.com/identity-manager/kb/290330/how-to-configure-settings-as-per-the-system-information-overview, which outlines the System Information Overview available within One Identity Manager.

> **NOTE:** In virtual environments, you must ensure that the VM host provides performance and resources to the database server according to system requirements. Ideally, resource assignments for the database server are fixed. Furthermore, optimal I/O performance must be provided, in particular for the database server. For more information about environment virtualization, see One Identity's Product Support Policies.

Requirements for a managed instance in Azure SQL Database

For more information about Azure SQL Database, refer to the Microsoft website under https://azure.microsoft.com/en-us/products/azure-sql/database/.

The following requirements and limitations apply to the use of a managed instance in Azure SQL Database as a database system.

- The **Business Critical** tier is required.
- Ledger is not supported. For more information, see the Knowledge Base.

Requirements for Azure SQL Database as database system

For more information about Azure SQL Database, refer to the Microsoft website under https://azure.microsoft.com/en-us/products/azure-sql/database/.

The following requirements and limitations apply to the use of Azure SQL Database as a database system.

- If you use Azure SQL Database as the database system, you must supply a database. There is no support for creating a new database in Azure SQL Database with the Configuration Wizard.
- `use` statements are not supported.
- Strong passwords must be used for the SQL login.

  For more information, see under Strong Passwords in the Microsoft documentation.
- Ledger is not supported. For more information, see the Knowledge Base.

Requirements for Amazon RDS for SQL Server as database system

The following requirements and limitations apply to the use of Amazon RDS for SQL Server as a database system.

- Ledger is not supported. For more information, see the Knowledge Base.
- The granular permissions concept is not supported.

Minimum requirements for administrative workstations

A minimum of the following system prerequisites must be fulfilled before installing the One Identity Manager components on an administrative workstation.

Table 28: Minimum system requirements for administrative workstations

Requirement	Detail
Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	5 GB
Operating system	Windows operating systems Following versions are supported: • Windows 11 • Windows 10 (64-bit) with at least version 1511
Additional software	• .NET 10.0 SDK • Microsoft Edge WebView2
Supported browsers	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimum requirements for the Job server

A minimum of the following system prerequisites must be fulfilled to install the One Identity Manager Service on a server.

Table 29: Minimum system requirements for Job servers

Requirement	Detail
Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 Linux operating systems • Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems • .NET 10.0 Desktop Runtime **NOTE:** Take the target system manufacturer's recommendations for connecting the target system into account. Linux operating systems • .NET 10.0 Runtime **NOTE:** It is recommended to use .NET container images.

Minimum requirements for API Servers

A minimum of the following system prerequisites must be fulfilled to install an API Server.

Table 30: Minimum system requirements for API Servers

Requirement	Detail
Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 Linux operating systems • Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems • ASP.NET Core 10.0 Windows Hosting Bundle • Microsoft Internet Information Services 10, 8.5, or 8 with the server roles: • Web Server > Common HTTP Features > Static Content • Web Server > Common HTTP Features > Default Document • Web Server > Application Development > ISAPI Extensions • Web Server > Application Development > ISAPI Filters • Web Server > Application Development > WebSocket Protocol • Web Server > Security > Basic Authentication

Requirement	Detail
	- Web Server > Security > Windows Authentication - Web Server > Performance > Static Content Compression - Web Server > Performance > Dynamic Content Compression Linux operating system - ASP.NET Core 10.0 Runtime **NOTE:** It is recommended to use .NET container images. - ASP.NET Core 10.0 Hosting process manager, deployed via Docker container

Minimum requirements for the application server

A minimum of the following system prerequisites must be fulfilled for installation of the application server.

Table 31: Minimum system requirements for application servers

Requirement	Detail
Processor	8 physical cores 2.5 GHz+
Memory	8 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: - Windows Server 2025 - Windows Server 2022 - Windows Server 2019 - Windows Server 2016 Linux operating systems

Requirement	Detail
	• Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems • ASP.NET Core 10.0 Windows Hosting Bundle • Microsoft Internet Information Services 10, 8.5, or 8 with the server roles: • Web Server > Common HTTP Features > Static Content • Web Server > Common HTTP Features > Default Document • 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 operating system • ASP.NET Core 10.0 Runtime **NOTE:** It is recommended to use .NET container images. • ASP.NET Core 10.0 Hosting process manager, deployed via Docker container

Supported data systems

This section lists the data systems supported by One Identity Manager connectors in this version.

Table 32: Supported data systems

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.
Connector for relational databases	Any relational databases supporting ADO.NET. **NOTE:** Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer.
Generic LDAP connector	Any LDAP directory server conforming to version 3. The LDAP connector requires the directory server to be RFC conform. Specifically, to conform to the standards RFC 4514 (Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names) and RFC 4512 (Lightweight Directory Access Protocol (LDAP): Directory Information Models). **NOTE:** Other schema and provisioning process adjustments can be made depending on the schema.
Active Directory connector	Active Directory shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, and Windows Server 2025.
Microsoft Exchange connector	• Microsoft Exchange server 2016 with the latest cumulative update • Microsoft Exchange server 2019 with the latest cumulative update • Microsoft Exchange Server Subscription Edition (Exchange Server SE) • Microsoft Exchange Hybrid environments
SharePoint connector	• SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition

Connector	Supported data systems
SAP R/3 connector	• 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, and 7.69 • SAP ECC 5.0 and 6.0 • SAP S/4HANA On-Premise Edition 1.0 and 2.0 as from SAP BASIS 7.40 SR 2 and 7.50 (also for installing with SAP BASIS 7.53) • SAP S/4HANA Cloud 2022 and 2023 with SAP BASIS 7.57 and 7.58 • SAP Connector for Microsoft .NET 3.1 for 64-bit with at least version 3.1.5 (compiled for .NET (formerly .NET Core))
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the specifications for Safeguard Authentication Services.
Domino connector	• HCL Domino Server versions 12 and 14 • HCL Notes Client versions 12.0.1 (only 64 bit) and 14.0 The same major version is used for the HCL Domino Server and the HCL Notes Client.
Generic database connector	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • SAP HANA • PostgreSQL
Mainframe connector	• RACF • IBM i

Connector	Supported data systems
	• CA Top Secret • CA ACF2
PowerShell connector	• PowerShell Version 7.x or later
Active Roles connector	• One Identity Active Roles 8.0, 8.1.1, 8.1.3, 8.1.5, and 8.2.1
Microsoft Entra ID connector	• Microsoft Entra ID **NOTE:** Synchronization of Microsoft Entra ID tenants in national cloud deployments with the Microsoft Entra ID connector is not supported. This affects: • Microsoft Cloud for US Government (L5) • Microsoft Cloud Germany • Microsoft Entra ID and Microsoft 365 operated by 21Vianet in China The Chinese cloud deployment operated by the Microsoft partner 21Vianet is only available for test purposes and is not supported. For more information, see https://support.oneidentity.com/KB/312379. • Microsoft Teams
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0. They must conform to RFC 7643 (System for Cross-domain Identity Management: Core Schema) and RFC 7644 (System for Cross-domain Identity Management: Protocol).
Exchange Online connector	• Microsoft Exchange Online

Connector	Supported data systems
Google Workspace connector	• Google Workspace
Oracle E-Business Suite connector	• Oracle E-Business Suite version 12.1, 12.2, 12.2.10, 12.2.11, 12.2.12, and 12.2.13
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard version 8.0 and 8.1 You can find the PowerShell module to match each supported version in the `Modules\PAG\dvd\AddOn\safeguard-ps` directory on the One Identity Manager installation medium. Versions without a matching PowerShell module on the One Identity Manager installation medium are not supported.

Long Term Support (LTS) and Feature Releases

You can choose between two paths for receiving releases: Long Term Support (LTS) Release or Feature Release.

Long Term Support (LTS)

- The One Identity Manager LTS version is 10.0. For all LTS releases of One Identity Manager, the first digit identifies the release and the second is always a zero (for example, 10.0).
- Maintenance LTS Releases (known as Cumulative Updates): A third digit is added; for example, 10.0.1.

Feature Release

- Feature Releases' version numbers are two digits (for example, 10.1, 10.2, 10.3 etc).

The table below shows a comparison of Long Term Support (LTS) Release and Feature Release.

Table 33: Comparison of Long Term Support (LTS) Release and Feature Release

Category	Long Term Support (LTS) Release	Feature Release
Release frequency	Every 24 months (includes resolved issues and security related updates).	Approximately every 12 months (includes resolved issues and security related updates).
Duration of full support	24 months	12 months
Duration of limited support	12 months (after the end of full support)	12 months (after the end of full support)
Versioning	All versions where the second number is **0**. For example: 10.0.0 (10.0.1, 10.0.2,), 11.0.0, 12.0.0, and do on.	All versions where the second number is not **0**. For example: 10.1.0 (10.1.1, 10.1.2), 10.2, 10.3, and so on.
Duration of service pack availability between releases	Approximately every 6 months, cumulative updates (CUs) are expected for each LTS release.	Every 6 months patch releases (service pack) are expected for each feature release currently supported.
Criteria for issuing hotfixes for LTS outside of a cumulative update cycle	• The product is not functioning after installing the most recent CU and the customer cannot wait until the next CU is available. • The product is not functioning/is inoperable which is causing a production outage/serious issue. • A security related fix is needed on a priority basis to address a vulnerability. • No fixes will be issued to implement an enhancement outside of the cumulative update cycle.	

Release details can be found at Product Life Cycle.

One Identity strongly recommends always installing the latest revision of the release path chosen by the customers/partners (Long Term Support path or Feature Release path).

Moving between LTS versions and Feature Release versions

You can move from an LTS version (for example, 10.0 LTS) by installing a later feature release or version (for example 10.3). Once this has happened, you are not on the LTS support path until the next LTS base version (11.0, etc.) is installed.

You can move from a Feature Release to an LTS Release, but only to an LTS release with a later version. For example, you cannot move from 10.3 to 10.0 LTS. You have to keep upgrading with each new Feature Release until the next LTS Release version is published. For this example, you would wait until 11.0 LTS is available.

Patches

For LTS, there are no patches released, only hotfixes, and these are distributed only in rare cases. Refer to the previous table for the criteria for LTS hotfixes. These hotfixes need to be applied in order of their release.

LTS has periodic cumulative updates (CUs) provided for LTS customers, which roll out the issues resolved during that period. It is not required to install every CU separately. For instance, if CU1 is released followed by CU 2, you do not need to install CU1 before installing CU2. The CUs are cumulative.

For more information, see the knowledge article 4372133.

For customers on the feature release option track, maintenance releases are cumulative, meaning that maintenance releases do not need intermediate releases to be installed to update to a newer maintenance release. This is unchanged from previous versions. For example, if you are using 10.1.1 and want to upgrade to 10.3 and versions 10.1.3, 10.1.4 and 10.1.5 have been released, you can simply install version 10.3, which will automatically apply the fixes from 10.1.3, 10.1.4 and 10.1.5.

Frequently Asked Questions (FAQs)

What is Long Term Support (LTS)?

- LTS is a support option that allows you to stay on the same release for an extended period of time while still receiving the high level of support that One Identity is known for. While on the LTS path, you receive updates aimed at resolving issues and vulnerabilities. There are not, however, any product enhancements or features delivered while on the LTS release.

What are the benefits to being on an LTS release?

- Some enterprises have a difficult time in keeping up with the migration to new releases in a timely manner to fit within the vendor’s support guidelines. This allows the enterprise to stay on one version for a considerable amount of time.

What are the disadvantages to being on an LTS release?

- The negatives, of course, are missing out on receiving the latest enhancements and features from the vendor.

Duration of an LTS release

- A Long Term Support (LTS) version provides you with up to 3 years of support after the original release date or until the next LTS release (which ever date is later); with an option to continue via Extended Security Support (ESS).

How do I make the move to the LTS support option?

- When you install an LTS version, such as One Identity Manager 10.0, you are automatically on the LTS path. The choice you make for the next release that you install, determines whether you remain on LTS or go to the traditional support model.

Once I choose to go on the LTS path, can I ever move back to the feature release path?

- Yes. You can do this by installing a later maintenance version or feature release. For example, if you currently have version 10.0 (LTS) and decide to move to 10.3, you will come off the LTS support path until you install the next base LTS version (11.0, etc.)

Is there an extra charge if I choose the LTS option?

- No, long term support is included in your annual maintenance renewal. An option to continue limited support is offered at an additional charge via our Extended Security Support (ESS).

Product licensing

Use of this software is governed by the Software Transaction Agreement found at https://www.oneidentity.com/legal/sta.aspx. This software does not require an activation or license key to operate.

This product does not require licensing.

Upgrade and installation instructions

To install One Identity Manager 10.0 for the first time, follow the instructions under Installing One Identity Manager. For more information, see Updating One Identity Manager.

> **IMPORTANT:** Note the Advice for updating One Identity Manager.

Advice for updating One Identity Manager

Take note of the following information when updating One Identity Manager.

- Test changes in a test system before you load a migration package into a production system. Use a copy of the production database for testing.
- Ensure that the administrative system user, who is going to compile the database, has a password before you update the One Identity Manager database to version 10.0. Otherwise, the schema update cannot be completed successfully.
- For One Identity Manager databases on SQL Servers, it is recommended, on performance grounds, that you set the database to the **Simple** recovery model for the duration of the schema update.
- During the update of a One Identity Manager database to version 10.0, different columns that were already semantically defined as mandatory fields become physical mandatory fields.

  During the schema update with the Configuration Wizard, errors may occur due to inconsistent data. The update quits with an error message.

  ```
  <table>.<column> must not be null
  ```

  ```
  Cannot insert the value NULL into column '<column>', table '<table>'; co
  lumn does not allow nulls.
  ```

  ```
  UPDATE fails
  ```

  Check and correct data consistency before updating a One Identity Manager database. In the add-on for the Configuration Module on the installation medium, a test script (`\SDK\SQLSamples\MSSQL2K\30374.sql`) is provided. In case it fails, correct the data and restart the update.
- One Identity Manager uses In-Memory OLTP (Online Transactional Processing) for memory-optimized data accesses. The database server must support Extreme Transaction Processing (XTP). If XTP is not enabled, the installation or update will not start. Check whether the SQL Server property **Supports Extreme Transaction Processing** (IsXTPSupported) is set to **True**.

  The following prerequisites must be fulfilled to create memory-optimized tables:

  - A database file with the file type **Filestream data** must exist.
  - A memory-optimized data filegroup must exist.

  The Configuration Wizard checks whether these prerequisites are fulfilled before the One Identity Manager database can be installed or updated. The Configuration Wizard offers repair methods for creating the database file and database group.
- During the update, calculation tasks are queued in the database. These are processed by the DBQueue Processor. Processing calculation tasks may take some time depending on the amount of data and system performance.

  This is particularly the case if you save large amounts of historical data in the One Identity Manager database, such as change data or data from process handling.

  Therefore, ensure that you have configured an appropriate procedure for archiving the data before you update the database. For more information on archiving data, see Change management.
- For the period of the update, the database is set to single user mode. Close all existing connections to the database before starting the schema update.

- You may experience problems activating single-user mode when using database mirroring.
- After the update has completed, the database switches automatically to multi-user mode. If this is not possible, you receive a message in which you can manually switch to multi-user mode.
- Once this version has been installed, users that need to access the REST API in the application server require the **Enables access to the REST API on the application server** (`AppServer_API`) function. Assign this program function to the users.
- Use the `Modules\QBM\dvd\AddOn\SDK\SQLSamples\MSSQL2K\SDK_Remove_Rights_on_msdb.sql` SDK script to remove permissions that are no longer required for the msdb database.
- It is not recommended to perform an upgrade of the existing modules to a new One Identity Manager version and install additional modules at the same time. This may cause dependencies between modules to be constructed incorrectly. First update the existing modules to the new One Identity Manager version. Then restart the Configuration Wizard and install the additional modules.

Updating One Identity Manager to version 10.0

> **IMPORTANT:** Note the Advice for updating One Identity Manager.

To update an existing One Identity Manager installation to version 10.0

1. Run all the consistency checks in the Designer in **Database** section.
   1. In the Designer, start the Consistency Editor with the **Database > Check data consistency** menu item.
   2. In the **Test options** dialog, click AZ↓.
   3. Under the **Database** node, enable all the tests and click **OK**.
   4. Start testing with the **Consistency check > Run** menu item.

      All the database tests must be successful. Correct any errors. Some consistency checks offer repair options for correcting errors.
2. Update the administrative workstation, on which the One Identity Manager database schema update is started.
   1. Run the `autorun.exe` program from the root directory on the One Identity Manager installation medium.
   2. Change to the **Installation** tab. Select the Edition you have installed.
   3. Click **Install**.

      This starts the installation wizard.
   4. Follow the installation instructions.

> **IMPORTANT:** On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise, the components are not updated and a new installation is created in the second directory instead.

3. Complete the One Identity Manager Service on the update server.
4. Make a backup of the One Identity Manager database.
5. Run the One Identity Manager database schema update.
    - Start the Configuration Wizard on the administrative workstation and follow the instructions.

      Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.
        - Use the same user as you used for initially installing the schema.
        - If you created an administrative user during schema installation, use that one.
        - If you selected a user with Windows authentication to install the schema, you must use the same one for updating.
6. Update the One Identity Manager Service on the update server.
    1. Run the `autorun.exe` program from the root directory on the One Identity Manager installation medium.
    2. Change to the **Installation** tab. Select the Edition you have installed.
    3. Click **Install**.

       This starts the installation wizard.
    4. Follow the installation instructions.

> **IMPORTANT:** On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise, the components are not updated and a new installation is created in the second directory instead.

7. Check the login information of the One Identity Manager Service. Specify the service account to use.
8. Start the One Identity Manager Service on the update server.
9. Update other installations on workstations and servers.

   You can use the automatic software update method for updating existing installations.

To update synchronization projects to version 10.0

1. If you have set up synchronization projects for connecting cloud applications in the Universal Cloud Interface, update the target system schema in these synchronization projects using the Synchronization Editor.
2. Any required changes to system connectors or the synchronization engine are made

available when you update One Identity Manager. These changes must be applied to existing synchronization projects to prevent target system synchronizations that are already set up, from failing. Patches are made available for this.

> **NOTE:** Some patches are applied automatically. A process that migrates all existing synchronization projects is queued in the Job queue to do this. To run the process, the One Identity Manager Service must be started on all synchronization servers.

- Check whether the process `DPR_Migrate_Shell` has been started successfully.

  If the patch cannot be applied because the target system could not be reached, for example, you can manually apply it.

For more information, see Applying patches to synchronization projects.

To update an application server to version 10.0

- The application server starts updating automatically after the One Identity Manager database schema update.
- To start the update manually, open the application's status page in the browser and select **Update immediately** from the current user's menu.

To update an API Server to version 10.0

- After updating the One Identity Manager database schema, restart the API Server. The API Server is updated automatically.

To update the Manager web application to version 10.0

- The previous Manager web application is no longer supported. Uninstall the Manager web application.
- Use the Manager web application provided through the API Server.
  - Enable the **Web Server > Application Development > WebSocket Protocol** server role for Microsoft Internet Information Services.
  - Install the **Server | Web | Business API Server | Manager** machine role.

Applying patches to synchronization projects

> ⚠ **CAUTION: Patches do not alter custom changes in synchronization projects. This means that conflicts may occur if patches are applied to synchronization projects that have been customized. It may cause loss of data.**
> ***Before you apply a patch***
>
> 1. Read the patch description to decide whether it provides the necessary improvements for the synchronization project.
> 2. Check whether conflicts with customizations could occur.

⚠

3. Create a backup of the database so that you can restore the original state if necessary.
4. (Optional) Deactivate the synchronization project.

NOTE: If you update existing synchronization projects, the connection parameters from the default variable set are always used. Ensure that the variables in the default variable set contain valid values.

NOTE: If you have set up synchronization projects for connecting cloud applications in the Universal Cloud Interface, update the target system schema in these synchronization projects before you apply the patches. Use the Synchronization Editor.

To apply patches

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Edit > Update synchronization project** menu item.
3. In **Available patches**, select the patches you want to apply. Multi-select is possible.

   In **Details - Installation summary**, all patches are displayed in order of installation.
4. Click **Apply selected patches**.
5. Enter any user input as prompted.
6. Use the patch log to check whether customizations need to be reworked.
7. If required, rework customizations in the synchronization configuration.
8. Run a consistency check.
9. Simulate the synchronization.
10. (Optional) Activate the synchronization project.
11. Save the changes.

NOTE: A patch does not take effect until the changes associated with it are saved in the database. If consistency check or simulation errors occur that cannot be corrected, you can dismiss the patch changes by reloading the synchronization project without saving the changes.

For detailed information about updating synchronization projects, see Updating existing synchronization projects.

Related topics

Verifying successful installation

To determine if this version is installed

- Start the Designer or the Manager and select the **Help > Info** menu item.

  The **System information** tab gives you an overview of your system configuration.

  The version number 2025.0012.0001.0000 for all modules and the application version 10.0 v100-338026 indicate that this version is installed.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe.

The release is localized in the following languages: German

This version has the following capabilities or constraints: Other languages, designated for the Web UI, are provided in the product One Identity Manager Language Pack.