One Identity Manager 9.2

Release Notes

29 September 2023, 10:58

These release notes provide information about the One Identity Manager release version 9.2. You will find all the modifications since One Identity Manager version 9.1.1 listed here. For the most recent documents and product information, see Online product documentation.

One Identity Manager 9.2 is a minor release with new functionality and enhanced behavior. See New features on page 2 and Enhancements on page 7.

If you are updating a One Identity Manager version older than One Identity Manager 9.1.1, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under One Identity Manager Support.

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

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

About One Identity Manager 9.2

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 automation-optimized 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 9.2:

General

- Support for Amazon RDS for SQL Server as a database system.
- A configuration library with variations of templates and formatting scripts is available. There are different templates supplied for the `CentralAccount`, `CentralEBSAccount`, `CentralSAPAccount`, `DefaultEmailAddress`, and `InternalName` columns in the `Person` table as well as formatting scripts.
- Automated monitoring of object changes

  After objects have changed in One Identity Manager, the processing of these changes can be monitored automatically via an interface (REST API). The REST API returns the resulting process ID for each object action. This process ID can be used to retrieve various information about the processes that handle the object changes.
- The functionality of the `FileComponent.ModifyFileAccess_DotNet` process task has been extended.

  A new parameter, `AccessControlList`, allows multiple entries of access permissions to be configured. The `ModifyFileAccess_Universal` process task has been replaced by this process task in the default processes.

IMPORTANT: In the processes to create home and profile directories for Active Directory user accounts, the **QER | Person | User | AccessRights | HomeDir | EveryOne**, **QER | Person | User | AccessRights | ProfileDir | EveryOne**, **QER | Person | User | AccessRights | TerminalHomeDir | EveryOne**, and **QER | Person | User | AccessRights | TerminalProfileDir | EveryOne** configuration parameters are no longer taken into account.

Ensure that the subdirectories under the root directories, such as the home directory, do not inherit permissions from the Everyone user group. Otherwise, there is a possibility that the user group obtains unwanted permissions on all home directories.

HTML web applications

NOTE: New Web Portal features have been implemented for the HTML application but not for the Web Designer Web Portal.

- The Web Portal offers context-sensitive help. This shows help texts and links to the user guides.
- The Web Portal now displays descriptions of certain properties as help.
- In the Web Portal, you can now compare identities and their properties with each other.
- In the Web Portal, you can now display responsibilities of identities that report to you. You can also limit the identities displayed to just those that have left or will soon leave the company.
- To make it easier to maintain entitlements required by a team, you can now create a role for the identities you are responsible for.
- **TECH PREVIEW ONLY**: The Web Portal supports editing of approval workflows.

  NOTE: This feature is only available to users who have the **Portal_Preview_ WorkflowEditor** program function.
- The Web Portal now shows approval guidance for pending requests.
- The Web Portal can now display archived requests.
- In the Web Portal, you can now display approval guidance for pending attestation cases.
- You can now edit policy collections in the Web Portal.
- There is now a feature in the Web Portal that provides recommendations for assigning entitlements to departments, application roles, business roles, cost centers, locations, or system roles.
- In the Web Portal, those responsible for a software application now see the identities that have access to the software application.
- In the Web Portal, you can now link and use custom designs.
- In the Web Portal, you can now maintain translations of application names and descriptions.

- In the Web Portal, you can now use search terms as filters. To do this, you enter the desired term in the search field and then press the **Enter** key.
- In the Operations Support Web Portal, you can now display the contents of the DBQueue.
- The Operations Support Web Portal now displays pending objects only for target systems for which the user is responsible.
- In the Operations Support Web Portal, you can now see the completed or still open operations in the system that belong to a specific process ID.
- In the Operations Support Web Portal, you can now display the operation history. Operations can be filtered by time, change type, and user that triggered it.
- In the Operations Support Web Portal, you can now view the process history.
- Log files can now be viewed and downloaded in the Administration Portal.

Target system connection

- Property mapping rules can be used to configure whether the order of the values of multi-valued schema properties is taken into account when detecting rogue modifications.
- Extension of the RemoteConnectPlugin

  The RemoteConnectPlugin has been extended. Additional authentication methods can be used to establish a remote connection to the target system. Additional properties, such as timeout or certificates, can be configured.
- If system filters or object filters are created in the Synchronization Editor, it is possible to test whether the filter condition provides the correct results.
- Changes to virtual schema properties can be tested directly in the Synchronization Editor mapping editor.
- Support for Role-based access control (RBAC) and privileged identity management (PIM) for Azure Active Directory in new "RBAC" and "PIM" modes. Due to limitations of the Microsoft Graph API, the role management feature in One Identity Manager in "PIM" mode supports only the global directory space for active role assignments. These features must be activated manually.

  A patch with the patch ID VPR#35513 is available for synchronization projects.
- Additional identity management related schema properties are mapped to Azure Active Directory user accounts.

  A patch with the patch ID VPR#36729 is available for synchronization projects.
- Additional schema properties are mapped for the last login time of Azure Active Directory user accounts. These schema properties can only be accessed under an Azure Active Directory premium license.

  A patch with the patch ID VPR#33776 is available for synchronization projects.
- Support for hierarchical address books in Exchange Online.

  A patch with the patch ID VPR#35780 is available for synchronization projects.

- Support for Microsoft Teams team templates.
- Support for POSIX enhancements for Active Directory user accounts, groups, and contacts.

  Patches for synchronization projects with patch ID VPR#14634 and VPR#14634_ARS are provided.
- Support for hierarchical address books in Microsoft Exchange.

  A patch with the patch ID VPR#35779 is available for synchronization projects.
- Active Roles version 8.1.3 is supported to the previous extent.
- One Identity Manager supports the LDAP object class **eduPerson**. This object class is mainly used in directories of universities and colleges to simplify communication between institutions.
- Support for One Identity Safeguard versions 7.2 and 7.3.

  A patch with the patch ID VPR#36617 is available for synchronization projects.
- Support for One Identity Safeguard partitions.

  A patch with the patch ID VPR#36044 is available for synchronization projects.
- Support for SAP .Net Connector 3.1 for x64, with version 3.1.2.0 for Microsoft .NET 4.8 or later.
- Roaming of Notes user accounts is supported.

  A patch with the patch ID VPR#36087 is available for synchronization projects.
- The SCIM connector supports synchronization of SAP Cloud ALM applications via SAP Cloud Identity Services with the default schema. To set up the synchronization, you can use the **SCIM synchronization of the SAP Cloud ALM application** project template.
- Information is mapped about the last password change and the last login date of Unix user accounts.

  A patch with the patch ID VPR#36688 is available for synchronization projects.

Identity and Access Governance

- Renaming

  In the process of renaming, unused translations in the `DialogMultiLanguage` table have been cleaned up.

  - **Employees** to **Identities**

    One Identity Manager manages not only natural persons, but a wide variety of identity types. To represent this more clearly, the `Person` object type has been renamed from **Employee** to **Identity**. In the process, **Pseudo employee** has been renamed to **Virtual identity**.
  - **Request templates** to **Product bundles**

    - **Help desk calls** to **Tickets**
    - **Language culture** to **language** or **language code**
- Support for Behavior Driven Governance for One Identity Safeguard. This includes:
    - Attestation and recertification of memberships in PAM user groups for user accounts that have not made access requests within a defined period of time. The memberships are removed automatically if attestation is denied. The time period is set by the **TargetSystem | PAG | UnusedThresholdInDays** configuration parameter.
    - Detection of PAM objects, such as assets, user groups, or entitlements that have not been used for a defined period of time. If, according to the PAM audit log, an entitlement has not been used during this period, a recertification procedure can be used to determine whether the entitlement is still required. Unused entitlements can then be removed from the target system. The time period is set by the **TargetSystem | PAG | UnusedThresholdInDays** configuration parameter.
- New approval procedure **OX - Owner of the object in any request parameter of the request properties**.

  The approval procedure determines as approvers the owners (application role) of an object that is given in a request parameter. The application role is assigned to the object through a foreign key column. The name of the request parameter is given with the approval step, as well as the name of the table column that refers to the application role. The approval procedure can be used for all products that are assigned a request property that uses this request parameter.
- Terms of use can be allocated to attestation policies. The terms of use can be provided as a PDF file in different languages.
- In the Web Portal, attestors can be given approval recommendations. The recommendations for approving or denying attestation cases are calculated based on various criteria. The criteria are specified in the **QER | Attestation | Recommendation** configuration subparameters.

  NOTE: The feature has been implemented for the Web Portal HTML application but not for the Web Designer Web Portal.
- You can now assign additional properties to attestation cases.
- Attestation policies can be configured to generate an empty attestation run if no object to be attested is found when the attestation cases are calculated.
- New approval procedures **BA - Owner of the application** and **BE - Approver of application entitlement**

  The approval procedures determine the owner (application role) or approver (application role) of the associated application when attesting application entitlements in the Application Governance Module.
- New approval procedure **SP - Owner of service principal**

  This approval procedure determines the owner (application role) of the attested Azure Active Directory service principal.

See also:

- Enhancements on page 7
- Resolved issues on page 28
- Schema changes on page 49
- Patches for synchronization projects on page 57

Enhancements

The following is a list of enhancements implemented in One Identity Manager 9.2.

Table 1: General

Enhancement	Issue ID
The Update event is only generated if there were changes to the object.	30163
The UnitOfWork prevents object changes from being added after the commit is started, otherwise they would be lost.	35913
Introduction of a bulk query interface in the VI.DB, specifically to speed up front-ends.	36478
The Consistency Editor can filter consistency checks in the test options dialog.	32390
Improved the **DialogDeferredOperation with overdue actions, activated but without existing job** consistency check.	34789
The SQL formatter consistency check now also checks for correct parametrization of the `EmptyClause` for key columns.	35737
The **Objectkey references to non existing object (tolerated)** consistency check is no longer required and been removed.	37141
Enhanced performance and handling of autocompletion of syntax in script code.	35649
Improved function selection for calling scripts in the Designer Script Editor. The menu tries to preselect the script the respective selection.	36081
Improved how proxy view extensions are displayed in the Designer's Schema Editor.	36380
Improvements made to the user interface to support changes to multilingual translated data.	34794
Support for automatic translation of compound strings. This finds the translation of each part and combines them to form the completed string.	34477
In the Designer's Language Editor, customized default translations have a	36422

Enhancement	Issue ID
yellow background in the translation table.	
The format of the configuration data in the form definition have been reworked. Custom form definitions are converted automatically.	35422
The information in the `DialogLogicalForm.DialogFormDefinition` column are now check for valid XML notation when saved.	36125
Masking of free text variables in the user interface navigation has been improved. Users can now influence how special characters are masked when they use them.	35886
Using a script, user interface variables can be calculated dynamically and depending on the context. This allows display texts in the user interface to be context-sensitive.	36305, 36238, 36862
Implementation of a visibility script in diverse default methods. This hides the methods in the Manager's task menu if they cannot be run because of object specific conditions.	36509
The Manager shows a tool tip with a description on various assignment forms.	32033
A new control element enables the comfortable maintenance of complex data structures, which are stored on the database side, in the Json format or also in the .NET database ConnectionString format, for example.	35518
Improved accessibility of the hierarchical list control.	36640
The reason for denying a session certificate in the application server is now logged by NLog.	35618
The product version is now shown on the tile with system information in the application server.	35963
The `AppServer.Installer.CMD.exe` program is now installed locally in the same way as the other command line programs.	35894
It is now possible to edit an existing application server installation with the Web Installer.	33584, 314733
In the One Identity Manager Service log view, the **Raw Log** menu displays the NLog log including entries from plugins.	35763
The permissions for the Database Agent Service to access the **msdb** database that are no longer required, have been removed.	35337
The `DatabaseAgentServiceCmd.exe` program now writes all warnings and errors to the console output.	36134
The email configuration wizard can now specify a Job server that takes over the **SMTP server** functionality.	35564

Enhancement	Issue ID
When processes are generated for email notifications, error messages are logged if the relevant configuration parameters are not set or no valid email address is entered.	33690
Disabled Job servers are now better displayed in the Job Queue Info program.	35677
In the Job Queue Info, the stop and start behavior of the system (emergency stop) has changed to stop queue processing without a delay if possible.	36222
Improved how process step error messages are presented in the Job Queue Info program. A dialog with the entire error message can be opened via the error link or the context menu.	36918
Improved layout of buttons for emergency stop in the Job Queue Info toolbar.	37105
Logging in the database with NLog 5 is now possible.	36303
If an error occurs during saving, both the table name and the display name of the object are now output in order to better locate the faulty object.	36373
Improved output of error messages from the database.	36639
Autocomplete has been improved in the Object Browser filter.	36083
Extra space in the Object Browser filter text box has been removed.	36084
Enhanced performance importing cumulative transports with the Database Transporter.	36401
Improvements in the `DBTransporterCMD.exe` command line program.	37012, 37013
Various improvements to the Data Import program's user interface.	36611
The Software Loader displays a warning if the selected files for importing are not in a valid install directory.	35609
Enhanced support for horizontal read scale-out in local availability groups of an SQL Server cluster. • Templates for configuring read scale-out have been integrated into the application configuration files. • The different connection pools are now visible in the log.	36109, 36110, 36977, 37029
Enhanced performance for cleaning up the DBQueue Processor task buffer.	35978
There is now no process delivery if there are custom database triggers that are disabled.	36433
Columnstore indexes are excluded when a transport is created with the	36452

Enhancement	Issue ID
Database Transporter.	
Permissions on the `PersonPasswordHistory` table are removed if they are not required.	36940, 419127
Enhanced performance filling the `QBMSplittedLookup` table.	36973
The index weighting for the full-text search can now also be set for integer columns.	36801
Triggers are no longer disabled while the DBQueue is being compressed. This stops the database from switching into maintenance mode and there is no disadvantage to the users.	36975
For an HTML application, a database user can be specified whose has an access level that meets the required minimum of being able to use this HTML application.	36436
Enhanced performance of viewing conditions for different application roles.	36759
After a database migration, the data for the module definition of the customer module **CCC** is regenerated.	36820
Superfluous role definitions for the History Database have been removed. An SDK script is provided for creating the minimum required permissions.	35936
The Schema Extension allows custom columns to be deleted in the view tables.	36667
A report can be exported in a given format with just one click if it is configured correspondingly.	35607
The query and calculation settings for report parameters can be changed with the data dependencies script, the front-end will adapt automatically.	36573
Where clauses from the report definition of subscribable reports are now also marked as trusted.	36574
The System Debugger has new command line parameters `/Conn` and `/Auth` that allow login credentials to be passed directly, making it possible to login automatically.	36403
The `Quantum.MigratorCmd.exe` program can now be used to create custom permissions groups (`/Group` parameter) and run SQL statements after database installation (`/PostSQL` parameter).	35746
In the installation wizard, on the **Module selection** page, additional descriptions about each module are displayed when selected.	35830
A new authorization method has been implemented for using the RemoteConnectPlugin in Docker containers.	36454

Enhancement	Issue ID
Third-party components update.	36426
Increased security generating reports.	37255

Table 2: HTML web applications: Feature parity with the Web Designer Web Portal

Enhancement	Issue ID
In the Web Portal, it is now possible to save the current view of a page.	32356, 30242, 300743
In the Web Portal, you can now view statistics and KPIs, depending on the permissions of the logged-in user.	36789, 393878, 322309
In the Web Portal, the filter dialog has been revised and an option to create custom filters has been added.	206836
In the Web Portal, you can now send request inquiries to other identities.	250607
In the Web Portal, you can now display a state overview and a status comparison in the object history.	252817
In the Web Portal, you can now manage Webauthn security keys as long as the API Server is configured with RSTS.	259005
In the Password Reset Portal, you can now manage password questions.	277546
You can now sort tables in the Web Portal.	284241
In the Web Portal, you can now manage resources, assignment resources, multi-request resources, and multi-requestable/unsubscribable resources.	288423
In the Web Portal, it is now possible to create departments, application roles, business roles, cost centers, locations, and system roles.	288860
Managers, IT Shop administrators, and Compliance and Security Officers can view request from identities.	290759
In the Web Portal, you can now display the system entitlement history.	299095
In the Web Portal, you can now export tables.	300508
In the Web Portal, you can now display, create, and edit tickets.	304631, 305721
In the Web Portal, you can now edit the main data of risk index functions.	304675
In the Web Portal, you can now use function analysis to display identities with critical SAP functions that violate compliance rules. You can also use rule analysis to display compliance rules that include SAP functions and identify any identity that violates the compliance rules.	304676

Enhancement	Issue ID
Rule violation management has been extended in the Web Portal: • More details are displayed about rule violations. • Mitigating controls that are assigned to a rule violation are displayed. • Rule violation detection can be started manually.	305793
In the Web Portal, you can now filter by attestation cases in which a specific identity has made an approval decision.	305996
Auditors can now view identities in the Web Portal.	306003
In the Web Portal, Auditors can now view departments, application roles, business roles, cost centers, locations, and system roles.	306005
In the Web Portal, you can now display company policies.	306100
Compliance framework managers and auditors can now view compliance rules in the Web Portal.	308021
The Web Portal now requires explicit re-authentication of the logged-in user to agree to the terms of use. The authentication procedure for this is configurable and can be disabled.	314572
The Web Portal now supports browser notifications.	319194
In the Web Portal, you can now view and respond to request inquiries.	321526
In the Web Portal, you can now send inquiries about attestation cases to other identities.	321541
In the Web Portal, you can now view and respond to inquiries about attestation cases.	321542
In the Web Portal, those responsible for a software application can now edit the main data of the software application.	394940
Auditors now see all requests in the Web Portal.	400433
The Web Portal now displays list reports directly in the browser.	405305
The Web Portal now displays devices, and you can edit their master data.	405829, 275567
In the Web Portal, a request can now be resubmitted from the request history.	413040
The Web Portal displays information about the logged in user, their permissions groups, and program functions.	415628
The Web Portal displays the source data of certain statistics.	416009
In the Web Portal, you can now display policy violations associated with company policies.	416128

Enhancement	Issue ID
In the Web Portal, managers can now create individual delegations and deputizations for identities for which they are responsible.	420543
In the Web Portal, you can now see the mitigating controls assigned to company policies or policy violations. In the case of policy violations, you can also edit the mitigating control assignments.	421474
In the Web Portal, you can now display a hyperview of the logged in identity in the profile settings.	421695
In the Web Portal, you can now display hyperviews of objects involved in attestation cases and policy violations.	425269

Table 3: HTML web applications

Enhancement	Issue ID
It is now possible to edit an existing API Server installation with the Web Installer.	33584, 314733, 313398
During installation of the API Server it is possible to set the password of the default system user **IdentityRegistration**. It is also possible to specify another system user, whose login can be used to create new identities.	36343, 407727

The API Server can write the session ID to log entries.
To do this, there must be the following entry in the `<nlog>` section of the `nlog.config` file:
`<extensions>`
`  <add assembly="QBM.CompositionApi.Server" />`
`</extensions>`
	36902

Local customizing of an API Server configuration is now only allowed by default if the API Server was started from the command line on the `ImxClient`.
Local customizations are disabled on IIS-based installations. You can override this behavior by adding the following code snippet to the `web.config` file.
`<appSettings>`
`  <add key="IsStandAlone" value="true" />`
`</appSettings>`
	416938

The API Server supports Websocket API methods.	394642
Enhancements to API clients for Angular developers: • Named interfaces are now used for the parameter types. These interfaces are exported so that they can be used in the application	394386

Enhancement	Issue ID
code. • The parameter properties are stored with their descriptions in the API client.	
The API Server uses HTTP status code 403 if authentication fails.	405643
The SCIM API's CSRF protection mechanism of the API Server is disabled by default.	405926
API clients are now more stable if the network connection breaks.	264940
The API Server runs a version check. Access by API clients of other versions causes an error.	296243
Enhanced performance starting the API Server.	312481
Compatibility of the API Server with reverse proxies has been improved. Reverse proxies can be configured in the Administration Portal.	319175
The API Server uses less space for temporary files on an IIS installation.	328741
Type-safe classes are now supported for editing custom API plugins.	316845
The API Server now takes all languages into account that are listed in the `Accept-Languages` header of an API query.	316933
The `.WithSingleEntityRead()` extension method was implemented in the API Server. It can be used to load single entities via the API (identified by the primary key).	251366
If the base URL of the API Server does not match a web application, a corresponding log entry is now generated.	389277
Angular application debugging has been stabilized by implementing the `deleteDestPath` option.	407356
API client methods now support canceling of API requests.	390096
In the Administration Portal, naming of multiple configuration keys has been improved.	424491
Recently added configuration keys can now be deleted in the Administration Portal.	307180
The Administration Portal now displays the API documentation. You can also configure how the API documentation is displayed in the Administration Portal settings.	322436
Enhanced performance of the API documentation.	307709
Requests from the API documentation (Swagger) no longer fail due to the missing X-XSRF-TOKEN header, as it is now included in the requests.	394255

Enhancement	Issue ID
The SameSite cookie setting can now be edited in the Administration Portal.	386427
The domain of the cookies sent by the API Server can now be configured in the Administration Portal.	388463
A default design for web applications can now be configured in the Administration Portal.	322421
The web applications now support a high-contrast design.	316555
In the Administration Portal the `VI_ITShop_CanCloneCartItemsByPerson` and `VI_ITShop_CanCloneCartItemsByProduct` configuration parameters that have no effect, have been removed.	422641
Improved the Administration Portal display of the API Server status: • You can show the list of composition API caches. • You can empty the cache. • You can enable and disable cookies usage. • You can display charts on the start page that show the number of sessions in chronological order.	387864
In the Administration Portal, you can now configure that users cannot change the language in their profile settings and that the browser language is used for the web application interfaces instead.	35813, 206640
In the Administration Portal, you can now configure the maximum size of an identity's profile picture.	367838
The `ConfigFileEditorCMD` program now supports the `/preventdbupdate true` command line parameter. If this is set, the application token is not updated in the database. This parameter is primarily intended for use in containers.	405743
The Web Portal uses a new mode for searching products on the product selection page to provide more complete search results and enhance performance.	32800, 423711
When approving a request or an attestation case, the approval step in which the approval is being decided is now displayed.	34861, 316872
You can now specify values for request parameters of products assigned to a product bundle. These values are then pre-set from the corresponding product bundle on requesting.	33637, 316846
The user now receives a warning before saving and before starting an attestation policy if the expected number of attestation cases exceeds a given threshold. The threshold can be configured.	34918, 305302
The Web Portal has a completely revised **New Request** page.	35573, 312077

Enhancement	Issue ID
Enhanced performance in the Web Portal for: • approving attestation cases • displaying my responsibilities	35861, 36814
New attestation conditions are provided to identify unused user accounts, which can be used for attestation of user accounts and memberships in system entitlements.	37004
New attestation conditions are provided to identify unused PAM entitlements, which can be used, for example, as part of Behavior Driven Governance for One Identity Safeguard.	37005, 37006
In Web Portal, using the keyboard has been improved.	410172
IT Shop administrators can now edit product bundles in the Web Portal.	416274
In the Web Portal, you can now create a new system role for an application without assigning entitlements to this system role at the same time.	421193
Application entitlements of an application can now be filtered in the Web Portal.	425214
Enhanced editing of service items: • In the Web Portal, you can see which application the application entitlement of a service item is assigned to. • If the service item properties cannot be edited due to an application entitlement assignment, a message is displayed. • IT Shop administrators can change the owner of a service item.	292570
In the Web Portal, if SAP function compliance rules are violated, you can now display the SAP authorizations that lead to the rule violation.	297236
In Web Portal, you can now set certain properties for multiple products that you want to request at once (for example, validity and reasons).	309614
As a report administrator, you can now specify who can access or subscribe to a report in the Web Portal.	314124
You can now configure your own settings in the Web Portal: • Application design • Time zone • Using the profile language instead of the browser language	319031, 206656
Views in the Web Portal can now be configured on more pages: • Attestation runs • Rule violations	320784

Enhancement	Issue ID
• Identities overview in the Data Explorer • System entitlements overview in the Data Explorer	
When requesting from a product bundle in the Web Portal, the request parameters stored with the product bundle are now included as well.	322296
In the Web Portal, you can now zoom in and move around in hyperviews.	367241
In the Web Portal, you can now perform an origin analysis when attesting an assignment.	388598
In Web Portal you can now perform an origin analysis in the attestation history for an assignment attestation.	388599
In the Web Portal, you can now click to display hyperviews such that all the information is shown.	418561
If an attestation is approved or denied, an evaluation is carried out as to whether a reason must be provided.	415322
Hyperviews in web applications now support displaying of visual separators.	206664
The Web Portal and the Password Reset Portal now support a layout that hides the header and the menu bar.	404198
As the person responsible for an application, you can now edit the service category structure for the application in the Web Portal. A service item with application entitlement can now only be assigned to a service category under the basic service category of the application.	405217
A new menu item **Responsibilities > My Responsibilities** has been added in the Web Portal. You can now use this menu item to display all objects for which you are responsible.	406577
In the Web Portal, resolving rule violations of compliance rules for SAP functions has been improved.	320932
If role memberships of a logged-in user change, the user is notified in the Web Portal and must log in again.	293389
In the Web Portal, if you click an object for further editing or a detailed view, the pane that opens now shows the name of the corresponding object as a subtitle.	303776
If the **MitigatingControlsPerViolation** configuration parameter is set, the request approver can now add mitigating controls to the resulting rule violations of a request as long as the approver is also an exception approver for the violated rule. In addition, the user can now see the request's mitigating controls in the request history.	305815

Enhancement	Issue ID
If the **MitigatingControlsPerViolation** configuration parameter is set, you can now add mitigating controls to rule violations.	367357
Attestation runs that were started via a policy collection are now marked accordingly in the Web Portal.	316985
In the Web Portal, you can now cancel requests to which you have write permissions.	36058, 319102
Handling of pending attestation cases has been expanded to include the following: • Displaying terms of use for an attestation case if the terms of use have been assigned to the underlying attestation policy • Displaying policy violations of the attestation case base object • Attestation cases with policy violations are highlighted in the overview • Displaying mitigating controls for policy violations of an attestation case • Risk assessment of the attestation case basic object	319199
In the Web Portal, you can now assign mitigating controls to a policy violation.	319201
In the Web Portal, the display of selected objects has been standardized.	320942
Resolving rule violations has been expanded to include the following: • The user can specify a reason that will be used to unsubscribe requests if at least one unsubscription is made. • Generated unsubscriptions are displayed in the request history in such a way that it is apparent who resolved the rule violation. • A default reason is automatically used for request cancellations, indicating that the cancellation was made to resolve a rule violation.	321559
Hyperviews are now provided in the Web Portal for the following objects: • Identities • Departments • Application roles • Business roles • Cost centers • Locations • System roles • User accounts	367240

Enhancement	Issue ID
• Resources • Multi-request resources • Multi requestable/unsubscribable resources • Assignment resources • System entitlements • Compliance rules • Company policies	
In the Web Portal, you can display the history of an object chronologically.	417844
You can now use the Password Reset Portal to create a new user account.	387948
In the Web Portal, you can now manage the ticket attachments (download, upload, edit, and delete) as well as edit the structure of the attachment folders.	388586
In the Web Portal, you can now view your own attestation status.	388600
How the recipient of a delegation is displayed in the request history has been improved.	36122, 388967
The following program functions have been introduced. • Portal_UI_ApplicationAdmin • Portal_UI_ApplicationOwner • Portal_UI_PAGStatistics • Portal_UI_PasswordHelpdesk • Portal_UI_PersonAdmin • Portal_UI_PersonManager • Portal_UI_PersonStatistics • Portal_UI_PolicyAdmin • Portal_UI_PolicyOwner • Portal_UI_PolicyStatistics • Portal_UI_QERPolicyAdmin • Portal_UI_QERPolicyStatistics • Portal_UI_ResourceAdmin • Portal_UI_RoleAdmin • Portal_UI_RoleStatistics • Portal_UI_RuleStatistics • Portal_UI_ShopAdmin	395043, 427871

Enhancement	Issue ID
• Portal_UI_ShopStatistics • Portal_UI_StructAdmin • Portal_UI_StructStatistics • Portal_UI_TSBStatistics	
You can now specify in a parameter definition (for reports or requests) that the selection of a parameter value is made from a flat list (instead of from a tree).	307699
In the Operations Support Web Portal, the **Availability check** has been extended and revised.	205400
In the Operations Support Web Portal, only objects that are directly assigned are marked as outstanding.	316548
Displaying processes in the Operations Support Web Portal has been improved: • You can use the process ID to go directly to the operations that belong to the process ID. • You can see a summary status for each process. • You can see the list of objects affected by a process. • You can see the error message of a failed process step and copy it to the clipboard for further use.	327062
In the Operations Support Web Portal, the stop and start behavior of the system has changed to stop queue processing without a delay if possible.	393858
The Operations Support Web Portal is now only offered if a database connection with the **Configuration user** access level is used.	
The Angular applications now use Angular 14.	394843
The RSTS has been updated to version 2023-02-28.1. Changes: • Multiple instances of the service can be installed next to each other. • Integration of OneLogin MFA. • Support for LDAPS with SSL/TLS when connecting to Active Directory or an LDAP server. • New support for automatic monitoring and updating of metadata when configuring with a URL. • Starling 2FA removed. The RSTS must be uninstalled/reinstalled for the update.	404168

Table 4: Web Designer web applications

Enhancement	Issue ID
Third-party components JQuery UI and Angular.js updated.	315799, 417517
Enhanced performance in the Web Designer Web Portal displaying the shopping cart.	33913, 430424
When rule violations are resolved in the Web Designer Web Portal, the reason and the person who unsubscribed are now given for unsubscribed entitlements.	35754
Increased the Web Designer Web Portal's security.	36328, 430932, 415297
Increased security generating reports.	37244

Table 5: Target system connection

Enhancement	Issue ID
Support for using a connection certificate to log in to Azure Active Directory. This requires an X.509 certificate including private key. You can use a self-signed certificate. A patch with the patch ID VPR#36596 is available for synchronization projects.	36596
Service principals can now be assigned as owners of Azure Active Directory service principals. A patch with the patch ID VPR#35769 is available for synchronization projects.	35769
The list of permitted values of the preferred single sign-on mode for Azure Active Directory service principals has been extended.	37198
It is now also possible to remove Exchange Online distribution lists if the synchronization user account is not given in the distribution list as a manager.	36060
The Exchange Online connector now uses and requires the Exchange Online PowerShell module with version 3.2.0 or later.	36363
The maximum configurable number of simultaneous connections has been increased to **999** in the Exchange Online connector.	36521
The connector for Azure Active Directory and Microsoft Teams now uses version 5 of the Microsoft Graph .NET SDK (Graph Wrapper).	36738
Enhanced performance when loading Microsoft Teams teams and channels as part of synchronization.	33471

Enhancement	Issue ID
The **Allow members to create private channels** option is read in and synchronized for Microsoft Teams teams.	36568
When a Microsoft Teams team is archived, all associated properties except for custom columns are now locked and can no longer be edited.	36623
The connector for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019 now supports access to the `MessageCopyForSendOnBehalfEnabled` and `MessageCopyForSentAsEnabled` properties. There is no mapping in the default.	35784
Support for send-as permissions for Microsoft Exchange mail-enabled distribution groups. A patch with the patch ID VPR#35776 is available for synchronization projects.	35776
OneLogin roles can now be automatically added to the IT Shop. The behavior is regulated by the **QER | ITShop | AutoPublish | OLGRole** configuration parameter.	35878
In the case of OneLogin user accounts, it can only specify whether the user account is locked.	35989
If an exact change date for OneLogin user account can be set, the current timestamp is used as the revision counter.	37120
To support One Identity Safeguard Behavior Driven Governance, audit logs are synchronized. A patch with the patch ID VPR#36315 is available for synchronization projects.	36315, 36920
Support for PAM access requests for remote desktop applications for assets.	35731
Support for OneLogin as authentication provider for PAM user accounts. The reports and policies for using multi-factor authentication have been adapted accordingly.	35731
Support for PAM access requests for API keys for accounts.	36617
Clear up of the synchronization configuration for SAP authorization objects. A patch with the patch ID VPR#35904 is available for synchronization projects.	35904
The object filter can filter SAP user accounts by the feature `USTYP`.	36427
In the Unified Namespace, the mapping of object properties from SAP roles to system entitlements has been changed. `SAPRole.RoleDescription` is now mapped to `UNSGroup.Description`.	36498
A synchronization project for the synchronization of BI analysis author-	36514

Enhancement	Issue ID
izations can only be set up if the SAP Business Warehouse component is installed in the SAP R/3 system.	
When single roles are assigned to composite roles in the SAP R/3 system, only memberships marked as active are synchronized.	36766
When establishing the system connection to a cloud application, the number of items per page can be configured for object list requests. A patch with the patch ID VPR#36376 is available for synchronization projects.	36376
Improved user navigation in the project wizard when setting up synchronization with a cloud application with OAuth authentication.	36905
If a cloud application blocks access to the target system because too many requests are made, the SCIM connector attempts to resend the requests after a specified delay. Definitions according to RFC 6585 are observed. The connector retries up to 30 times.	36339
The SCIM connector allows customized lines in GET request headers.	36202
When the SCIM connector is authenticated via OAuth, the configured client ID and client secret data is always transmitted in the header and body of the `POST request`.	36912
The One Identity Manager connector provides a virtual schema property that can be used to map translations of single values.	36375
When setting up synchronization with the CSV connector, the path to the CSV file can be specified as an absolute path or as a relative path to the CSV system file. This way CSV files from different locations can be used in one synchronization project.	35420
The Powershell connector definitions consistency check now checks whether at least one return command (ReturnBinding) has also been defined for a property that is readable according to the definition.	35654
Advanced logging modes when running Windows PowerShell scripts with PowershellComponentNet4.	36811
Support for new format of ClientSecret strings generated by One Identity Starling Connect.	36156
Improved error handling for target system connectors that use the local cache when individual objects cannot be loaded due to corrupted data.	36793
The value of quota variables can also be specified as a percentage.	36510
Enhanced performance when creating display values for synchronization objects.	36284

Enhancement	Issue ID
The target system browser provides the option to edit a previously defined filter for the result list.	36154
The dialog for decrypting connection data in Synchronization Editor has been improved.	36026
In the dialog for selecting the synchronization server, an existing Job server can now also be selected. This automatically assigns the server function matching this Job server.	35903
If in Manager on the **Target system adjustment** form a method for handling the pending objects cannot be run due to constraints, the respective icon is disabled. Details about the respective constraint can be displayed.	31890
New consistency check for synchronization projects that warns about configuration errors in mappings of M:all tables (for example `ESetHasEntitlement`).	36666
Creating, changing, and deleting user accounts in custom target systems (`UNSAccountB`) avoid unnecessary post-processing tasks.	36989
New configuration parameter **QER | Person | User | DeleteOptions | DeleteOutstanding** which allows user accounts marked as pending to be deleted automatically.	32052
In the Manager, the **Define search criteria for identity assignment** form for target systems, now also displays the activation status of identities and user accounts. An option is provided to manually connect even locked user accounts to identities.	32254
In the Manager, inactive identities can now also be assigned to user accounts on the user account main data forms of the target systems. The new configuration parameter **QER | Person | HideDeactivatedIdentities** specifies whether inactive identities are shown or hidden on the user account main data forms.	36703, 36734
References to the Active Directory edition have been removed from the installation wizard and guides. Existing installations of this edition are not affected.	36939
The Manager overview forms for user accounts display information about heritability of system entitlements better.	36049

Table 6: Identity and Access Governance

Enhancement	Issue ID
The terms of use can be provided as a PDF file in different languages.	31889
The data about an attestation object of an attestation case is provided as a	35498

Enhancement	Issue ID
report or as a snapshot. Report and snapshot can be displayed in the Manager.	
Various enhancements determining attestors with the **SO** approval procedure.	36477
If compliance rule violations are identified in the request approval process, exception approvers may assign mitigating controls when approving the rule violation.	21081
Various columns in the `ComplianceRule` table have been additionally labeled as multi-language. Their contents can now be translated.	36845
The Rule Editor for compliance rule reworked for future extensions. This modification removed the assembly value in the XML configuration. Rule conditions created with older One Identity Manager versions can still be loaded. Compliance rule created with One Identity Manager 9.2 do not work in older One Identity Manager versions.	35131
Multifactor authentication can be requested for accepting terms of use.	35859
IT Shop customizer error messages use custom display values and date formats and can be translated.	36053
Email notifications will no longer be sent to permanently inactive identities.	36152
Service item attestators see all the information about an attestation object on the service items overview form.	36173
The overview form of an application role also displays the approval workflows in which the application role is determined to be the fallback approver.	36213
Deputizations and delegations come to an end when the deputy is deactivated.	36300
The display values of some values of the `AttestationHistory.DecisionType` column have been corrected so that the display value and the English translation of the display value are identical.	36460

Value	Previous display value	New display value
Abort	Aborted	Canceled
Direct	Direct	Forward
RevokeAdditional	RevokeAdditional	Revoke additional approver

If you retrieve translations of values in custom scripts, for example in email

<table>
<tr><th>Enhancement</th><th>Issue ID</th></tr>
<tr><td>notifications, adjust these scripts accordingly. Use the new display value as a key for the translation.
Example of use in the pre-script to generating a process:
• Previous: <code>Connection.MultiLanguage.GetInLanguage ("AttestationHistory", "DecisionType", "Abort", personLanguage).ToString()</code>
• New: <code>Connection.MultiLanguage.GetInLanguage ("AttestationHistory", "DecisionType", "Canceled", personLanguage).ToString()</code></td><td></td></tr>
<tr><td>The display values of some values of the <code>PWODecisionHistory.DecisionType</code> column have been corrected so that the display value and the English translation of the display value are identical.
<table><tr><th>Value</th><th>Previous display value</th><th>New display value</th></tr><tr><td>Abort</td><td>Abort</td><td>Cancel</td></tr><tr><td>AddAdditional</td><td>AddAdditional</td><td>Additional approver</td></tr><tr><td>AddHistoryEntry</td><td>AddHistoryEntry</td><td>Show in history</td></tr><tr><td>AddInsteadOf</td><td>AddInsteadOf</td><td>Delegation</td></tr><tr><td>ChangeBoard</td><td>ChangeBoard</td><td>Change shelf</td></tr><tr><td>CreateOrder</td><td>CreateOrder</td><td>Stock request</td></tr><tr><td>Grant</td><td>Grant</td><td>Approval</td></tr><tr><td>ResetReservation</td><td>ResetReservation</td><td>Reset reservation</td></tr><tr><td>RevokeAdditional</td><td>RevokeAdditional</td><td>Revoke additional approver</td></tr><tr><td>RevokeDelegation</td><td>RevokeDelegation</td><td>Revoke delegation</td></tr></table>If you retrieve translations of values in custom scripts, for example in email notifications, adjust these scripts accordingly. Use the new display value as a key for the translation.
Example of use in a script:
• Previous: <code>multiLanguage.Get("PWODecisionHistory", "DecisionType", "Grant")</code>
• New: <code>multiLanguage.Get("PWODecisionHistory", "DecisionType", "Approval")</code></td><td>36460</td></tr>
<tr><td>The request overview form displays the request properties that are used</td><td>36652</td></tr>
</table>

Enhancement	Issue ID
(modern definition) and their parameters.	
The **Request History** report for an identity now shows approved multi-request resources under the **Approved multi-request resources** tab.	36654
Calculation of SAP functions optimized.	36796
A reason can now be entered for the temporary deactivation of an identity. For this purpose, a `LeaveofAbsenceReason` (**Reason for absence**) column has been added to the `Person` table.	35739
Enhanced performance calculating SAP functions.	36821
Masked special characters can be used in the authorization definition of SAP functions.	36780
Enhanced performance in attestation policy condition testing.	37134
Improved how the **Move products** dialog is presented in the Manager.	36636
The following scripts for formatting links in emails to directly approve requests or directly attest, or for displaying rule violations have been converted internally to use `IEntity`. • VI_BuildITShopLinks • VI_BuildAttestationLinks • VI_BuildComplianceLinks If these scripts are to be custom used for any other purpose than for mail templates, the calling parameter must be changed from `Base` to `Entity`.	36556
The calculation of permitted approvers in the approval workflow has been optimized. Approval levels that have already been completed are no longer recalculated after each change.	35602
The **ApplicationStart_ApplicationGovernance** program function is no longer needed and has been removed.	35869
The **OA** and **TO** approval procedures have been extended to determine approvers for assignment requests. The **EN** approval procedure has been extended to determine attestors for assignments of system entitlements to hierarchical roles.	36432
If an email notification from the IT Shop cannot be sent due to a processing error, the sender of the email is informed and the original email is deleted from the outbox. A new mail template **Approval - Error processing an approval mail** is provided.	21300, 31884
When calculating the peer group factor, resources that can be requested more than once are also taken into account.	35854

See also:

- Schema changes on page 49
- Patches for synchronization projects on page 57

Resolved issues

The following is a list of issues addressed in this release.

Table 7: General

Resolved issue	Issue ID
Under certain conditions, hyperlinks are not fully displayed in the Mail Template Editor.	35676
In rare cases, an attempt was made during process handling to enter the same process more than once in the process display (`DialogProcess` table). This led to a primary key violation and consequently to the error.	35765
Error displaying dates in the Where clause wizard when they are given with **null** values.	35801
When editing the connection string in the connection dialog, the first change is ignored.	35911
In certain cases, an error occurs when database queries are run via the object layer. Error message: `the Size property has an invalid size of 0`	35993
When installing or updating One Identity Manager, custom files were saved in the wrong subdirectory.	36054
In the Script Editor of the Designer, the script list menu is too narrow.	36085
Error marking a completed process step for deletion or archiving.	36098
Error installing the application server due to Microsoft Edge WebView2 dependencies.	36107
The administrative user selected on the **System administrator permissions** page is not used in the Configuration Wizard.	36248
Cumulative transport packages are not displayed correctly in the transport history.	36260
Creating and setting up a One Identity Manager database requires an installation user with a **dbcreator** server role, even if a previously created database is going to be used.	36295
Process collection via **HttpJobProvider** does not work if SSL is configured	36329

Resolved issue	Issue ID
for use by the proxy server.	
In the Designer, if column definitions cannot be loaded in the Schema Editor if they were disabled via a preprocessor condition.	36340
Inconsistencies in the definition of DBQueue Processor task dependencies.	36366
In the Designer, the data source of a key value is not populated correctly in the Language Editor.	36402
Under certain conditions, when the DBQueue Processor replaces processes, entries are retained that reference processes that no longer exist.	36645
When changing the parameter type from calculation to user query, the **Table column (calc.)** column for the parameter (`DialogParameter.UID_DialogColumnCalculate`) is not cleared.	36664
Incorrect display of historical assignments in reports if a database view is used as table.	36695
If the Database Agent Service stops when DBQueue Processor tasks are being compressed, data is lost.	36708
The language code **nb** is missing.	36714
Incorrect conversion of time values with a time of `00:00` and a date format of `DateTime`.	36745
In the documentation about the Docker container for the One Identity Manager Service, the `CONFIGFROMDB` parameter is insufficiently described.	36779
Under certain conditions, there may be orphaned entries for deleted machine roles in the `ModuleInfo.xml` file of the **CCC** module after updating.	36810
An error sometime occurs in the system configuration overview. Error message: `Divide by zero error encountered.`	36822
In the One Identity Manager Installation Guide, port 443 is missing from the list of communication ports.	36851
Watch triggers are not created if a column for different database views is marked for logging data changes and the views are based on the same base table.	36857
In rare cases, a schedule is triggered several times.	36861
The Database Compiler stops responding when it is determining compiler tasks.	36865
An error occurs in Designer when assigning permission groups to applications.	36879

Resolved issue	Issue ID
Error message: `Object reference not set to an instance of an object.`	
An error occurs when calculating the display pattern if different data types are used. Error message: `Conversion failed when converting the nvarchar value '<value>' to data type int.`	36895
Users from time zones with UTC+00:00 are not able to log in to the Manager web application.	36901, 431158
Transport by change label does not transfer the description and comment of change labels.	36904
In reports created with the Report Editor, filters and summaries contain incorrect results.	36906
The comparison of columns with date and time values does not always work correctly.	36945
Error handling processes that use the `ModifyFileAccess_Universal` process task. Error message: `Cacls.Exe failed with return code 122 ("The data area passed to a system call is too small").` NOTE: The process task has been replaced by the `ModifyFileAccess_DotNet`process task. For more information, see New features on page 2.	36946
When upgrading from One Identity Manager version 8.x to a newer version, an error may occur when compiling the type-safe database model. Error message: `Keyword is not valid as an identifier.`	36949
Error saving an object change as a planned operation in the Manager if the Manager was started via an application server.	36951
Entries in the Job queue are often marked for recalculation. This blocks Job queue processing. The DBQueue Processor task `QBM-K-JobqueueOverviewInvalid` has now been replaced by a trigger.	36962, 36963
Performance issues testing for multi-column uniqueness if objects are added to the One Identity Manager database in bulk.	37027
It is not possible to assign SAP roles to SAP user accounts in the Manager web application.	37032, 431268
Error importing data into the `QBMDBPrincipal` table if it results in duplicate entries relating to database users or login names.	37045
Under certain conditions, recalculation tasks for the DBQueue Processor that relate to the Target System Base Module (TSB) are not automatically	37048

Resolved issue	Issue ID
deleted.	
Error displaying the `QBM_TransportToHistoryDatabase` process in the Process Editor if the **SQL processing server** server function is assigned to two Job servers or more.	37050
Changes to templates or formatting scripts in the Designer are not always saved in the database.	37056
An incorrect warning is displayed when opening a password policy in the Designer.	37083
Error if `DialogDatabase.EditionDescription` is marked as `isBlobExternal`.	37108
Filters generated in the SCIM connector may have an unnecessary bracket level. Some SCIM providers return a `Bad request` status due to these filters.	37119
The change history view of an object may exceed the IN clause limit of 8000 elements.	37140

Table 8: HTML web applications

Resolved issue	Issue ID
The Web Portal does not use the correct product names in the shopping cart.	35818, 317017
In the Web Portal, languages available for selection are not displayed in the respective language.	36138
The Docker container for the API Server does not log by Application Insights.	36484
The index in the Web Portal enters into an endless loop.	36587
In the Web Portal, clicking outside the request parameter prompt cancels the request.	36813
In the Web Portal, an error occurs when checking the shopping cart if the requested product has a request parameter that contains a list of permitted values.	36847, 431117
An error occurs in the Administration Portal when saving global changes.	36848, 431121
When approving delegations, an error occurs when a custom approval policy is used.	36854, 416803
Error testing request parameters in the shopping cart if the parameter contains a limiting condition with a variable.	36878
In the Web Portal, adding products to the shopping cart does not work.	37144
In the Web Portal, the request workflow displays withdrawal of an additional	292577

Resolved issue	Issue ID
approver incorrectly.	
If a user tries to log in to the password reset portal with an expired passcode, they get the wrong information.	305015
Under certain conditions, the Web Portal does not display the rule violation testing for assignment requests.	306828
In the Web Portal, under certain conditions, an error message is displayed during approval of an attestation case.	317836
In the Web Portal, if new requests are made through peer groups or reference users, the products selected through organizational structures are not added to the cart.	319781
Under certain circumstances, editing attestation policies in the Web Portal deletes the conditions of the attestation policy.	320926
The **Identity Access Comparison** report cannot be generated in the Web Portal.	322252
Under certain conditions, the Web Portal's search function does not work and generates an error.	327287
The Web Portal does not display all the details about a rule violation for a product that causes a rule violation when requested.	331942
In the Administration Portal, the values **true** and **false** are not translated.	386304
Stores assigned to shopping centers are not displayed in the list of editable stores in the Web Portal.	403983
The API Server creates a new session for each request if the same authorization token is used.	405848
Request parameters of type `query` are handled correctly only if the query column is either `XObjectKey` or a primary key column.	412932
Registering a new user in the Password Reset Portal fails.	415340
The Web Portal allows delegations to be created without a time limit.	416793
The search in the Administration Portal does not correctly handle upper and lower case letters.	418578
The process view in the Operations Support Web Portal displays all the process steps of a process with the same name.	419792
In the Operations Support Web Portal, existing Job queue tasks are only displayed with a delay.	426530

Table 9: Web Designer web applications

Resolved issue	Issue ID
In the `VI_Edit_Multiselect` component of the Web Designer, values cannot be cleared.	36558
Displaying an identity's main data causes an error in the Web Designer Web Portal.	36578, 405073
In the Web Designer Web Portal, it is not possible to unsubscribe a product.	36647
The Web Designer Web Portal does not show translation values in some menus.	36761, 414583
The Web Designer Web Portal does not identify a rule violation when the shopping cart is checked even though mandatory parameters are not populated.	36764, 431063
After logging off from the Web Designer Web Portal, redirection to the configured URI does not work if **Send redirect URI for the application** is configured in the OAuth/OpenID Connect configuration.	36874
When an approver opens and approves a request in the Web Designer Web Portal via a link, any existing valid-until date is deleted.	37121, 431359
Code copied to customized functions of the Web Designer is reformatted.	428028
In the `VI_Edit_Special_Person_TemporaryDeactivated` Web Designer component, the `IsTemporaryDeactivated` parameter cannot be set to **readonly**.	430791

Table 10: Target system connection

Resolved issue	Issue ID
The handling of outstanding Exchange Online email users generates unnecessary provisioning tasks for Azure Active Directory groups.	36707
Error synchronizing against the generic database connector when the synchronization server is set up on a Linux server. Error message: `The time zone ID 'FLE Standard Time' was not found on the local computer.`	34451
Error synchronizing with the One Identity Manager connector if virtual schema properties with the same name are used in schema types with the same name. Error message: `Error compiling synchronization project. An item with the same key has already been added.`	35811
Different OneLogin user account properties are changed by each synchronization.	35958
Performance problems synchronizing SharePoint Online with a lot of site	35975

Resolved issue	Issue ID
collections.	
In the Launchpad, an end user (database user) cannot enable offline mode for a target system.	36007
Error reading data with the CSV connector when there is a remote connection to the CSV system.	36126
Conversion error displaying Azure Active Directory objects in the target system browser. Error message: `[1777022] Schema property (extension_<guid>_description@User) only accepts data of type (System.String). The value loaded (["<user>"]) is however type (System.Text.Json.JsonElement).`	36306
Memberships in system entitlements that are marked as outstanding are in effect in the One Identity Manager. This means that the system entitlements in One Identity Manager cannot be deleted.	36395
In the schema extension file of an SAP R/3 schema, if a function is defined with optional parameters, the properties of each single object are populated with empty values during synchronization. However, in the target system browser, the properties are provisioned correctly.	36425
The One Identity Manager Administration Guide for Connecting to Unix Based Target Systems does not sufficiently describe the minimum permissions.	36435
`Insert` operations take unexpectedly long if the SCIM provider does not support searching for endpoints with filters.	36459
If the assignment of a BI analysis authorization to a BI user account is deleted in One Identity Manager, the provisioning process does not remove the assignment from the SAP R/3 system.	36517
The One Identity Manager Password Capture Agent Administration Guide does not describe the `DeleteJob` parameter.	36592
The One Identity Manager Administration Guide for Connecting to Exchange Online does not sufficiently describe the permissions for app-only authentication using a self-signed certificate.	36619
If several synchronization projects exist for a target system, the provisioning tasks might be generated incorrectly for the wrong (inactive) project.	36671
If a Microsoft Teams team is archived, the associated SharePoint Online page can still be edited.	36677
The One Identity Manager Administration Guide for Connecting to Microsoft Exchange does not sufficiently describe the required permissions.	36680

Resolved issue	Issue ID
SAP user account assignments to SAP roles are not updated correctly if the structure of the SAP roles changes.	36701
When using PowerShell module v3, an error may occur during synchronization with Exchange Online. Error message: `You must call Connect-ExchangeOnline before calling any other cmdlet.`	36709, 37137
When templates for mail-enabled Azure Active Directory groups are reused, it changes the `AADGroup.IsSecurityEnabled` and `AADGroup.IsMailEnabled` columns.	36713
The communication data of SAP user accounts is not read correctly from systems with business partner functionality. This happens if the user account is linked to an HCM person (identical personnel number) and separate address and communication data exist.	36754
Error accessing schema properties in the central database of synchronization projects for system synchronization that map M:N schema types or key resolutions. Error message: `The system (...) does not have a data store.` A patch with the patch ID VPR#36755 is available for synchronization projects.	36755
Sometimes the object properties of certain types of SAP R/3 schema extensions are all read correctly in the target system browser, but during synchronization not all properties are accessed.	36768
Missing customizer for OneLogin user accounts (`OLGUser` table).	36771
An error occurs if the value **$null** is returned when running a script with the `ExecuteScript` process task of the `PowerShellComponentNet4` process component. Error message: `Object reference not set to an instance of an object.`	36776
The `OLG_PersonAuto_Mapping_OLGUser` script references a non-existing column. Error message: `Column UID_TSBAccountDefUser does not exist.`	36788
Assigning group membership fails in an AIX system if there is no permission to use the `bin/mv` command.	36794
Error synchronizing owners of Azure Active Directory app registration if the owner is a service principal. A patch with the patch ID VPR#36799 is available for synchronization projects.	36799
Error loading a synchronization project.	36815

Resolved issue	Issue ID
Error message: `[System.TypeLoadException] Method 'TryConvertFromString' not found.`	
Error synchronizing Notes Admin4 databases and certificate requests. Error message: `Error running synchronization step (AdminRequest) of synchronization configuration (Initial Synchronization). Quota (2) exceeded for method (Delete object).` A patch with the patch ID VPR#36831 is available for synchronization projects.	36831
Delta synchronization does not enter the group type of Azure Active Directory groups correctly.	36840
Provisioning of Active Directory groups sporadically fails when memberships and the member are deleted at the same time.	36843
Error synchronizing an SAP R/3 environment if the synchronization configuration contains a schema extension that uses a Where clause longer than 72 characters in the table definition.	36869
Connection error in the SCIM connector when using authentication based on a client certificate, even though the certificate has been validated as correct.	36872
The overview form for Azure Active Directory user account displays disabled group memberships.	36899
In Azure Active Directory, loading user accounts without a picture can cause an `ImageNotFound` error.	36928
When loading faulty SAP user accounts, the synchronization quits instead of logging the faulty objects and continuing the synchronization.	36931
Under certain conditions, Active Directory synchronization fails with the error: `Value cannot be null.`	36938
If booking permissions are processed for an object that still has an element in Microsoft Exchange that is no longer a recipient itself, the error `You cannot call a method on a null-valued expression` occurs.	36953
Reading the `Tenant.AllowedDomainListForSyncClient` fails if the data for this property exist in SharePoint Online. Error message: `Object cannot be stored in an array of this type.`	36956
Error synchronizing SharePoint Online when a site collection contains a large number of sites. Error message: `The request uses too many resources.` A patch with the patch ID VPR#36961 is available for synchronization projects.	36961

Resolved issue	Issue ID
When synchronizing an SAP R/3 environment with revision filtering, not just the changed user accounts are loaded, all of them are. Error message: `Object list of type USER is not able to read property BAPIUCLASS~SYSID. Subsequent loading of all single objects will affect performance.` A patch with the patch ID VPR#36970 is available for synchronization projects.	36970
When loading a SCIM schema with schema extensions, the list of names of the schema extensions included is empty. A patch with the patch ID VPR#36985 is available for synchronization projects.	36985
Error in the generic database connector for Oracle Database when reading large numerical values from a table column of type `NUMBER(20)`. Error message: `Arithmetic operation resulted in an overflow`	36993
Error loading objects of the `ExternalEmail` schema type when the entire Google Workspace customer assigned as a member to a Google Workspace group.	37024
Error starting provisioning if there are object references for the changed object that were ignored during synchronization. Error message: `Unable to cast object of type 'System.Byte[]' to type 'System.IComparable'.`	37031
Incorrect conversion of date values in the generic database connector.	37037
Error in CSV connector when handling object references.	37039
Synchronizing memberships does not clean the synchronization buffer if **Ignore case** is enabled on the value comparison rule.	37062
On the main data forms of user accounts the values in the **Category** property are not displayed correctly.	37070
Delta synchronization of Azure Active Directory user accounts without a manager fails.	37088
In the `attributes` parameter of an HTTP `GET` request, the names of properties defined in an overlay file are not formatted according to RFC.	37099
Error in the RACF connector if the RemoteConnectPlugin is used.	37103
Error in the template for `OLGUser.status`.	37138
SAP schema extensions with nested Where clauses in the table definition do not return the expected data sets.	37146

Resolved issue	Issue ID
The log data from the database is not presented in the correct order in the system journal.	37155
Arbitrary changes to the `SAPComSMTP.SMTPAddr` column definition cause an error.	37169
The **DialogTable without Layout information** consistency check lists missing layout information for all custom tables.	37181

Table 11: Identity and Access Governance

Resolved issue	Issue ID
The default email address column template for identities (`Person.DefaultEmailAddress`) does not format values if neither the Microsoft Exchange Module nor the Domino Module are installed and active.	34915
If an approver can approve several approval steps at the same approval level, approval that is granted is not accepted although the **QER | ... | ReuseDecision** configuration parameter is set.	35517
Base objects for events on `PersonWantsOrg` and `AttestationCase` are not correct.	36430
The master data form for identities might prevent some interface elements in the Manager from being hidden due to an external error.	36485
If a product is moved to another shelf, renewal requests are not reset.	36634
In some cases, an error occurs when transporting approval workflows. Error message: `PWODecisionStep: Write permission denied for value "CountApprover".`	36641
Product owners of Exchange Online distribution groups are not removed from the application role.	36668
Viewing permissions for **VI_4_ALLUSER_LOOKUP** missing for Azure Active Directory service principals to request Azure Active Directory role eligibilities.	36710
In the Manager, the date for creating user accounts (`Person.TechnicalEntryDate`) cannot be set to the person's start date (`Person.EntryDate`).	36758
Permissions for the product owner **vi_4_ITSHOPADMIN_OWNER** missing for various tables.	36777
In the Manager, identities cannot be deleted or inserted in the results list of inactive identities.	36784
The auxiliary table for request procedures (`PWOHelperPWO`) sporadically contains duplicate entries.	36805

Resolved issue	Issue ID
Performance issues when processing DBQueue Processor tasks.	36826
On the overview form for an SAP composite role, the status of an assigned single role marked as pending is not displayed correctly.	36833
If exception approval is not permitted for a company policy, the **Checked** (`IsDecisionMade`), **Decision on** (`DecisionDate`), and the reason (`DecisionReason`) properties are no longer automatically set when policy violations are calculated.	36921
If products with a validity period (**Max. days valid**) are requested and the valid-until date is earlier than the end of the validity period, the valid-until date is automatically extended to match the length of the validity period.	36923, 431172
The `VI_MassDeleteDelegate` script fails with an error message if one of the requests has the status **Canceled**.	36924
Error in the `QER_PSlotResetOnInvalidRoot` procedure.	36955
Sporadic error in the `Created by QBMDBQueueProcess: handle object update for object type ITShopOrg` process. After being re-enabled, the process runs without errors.	36965
If a proxy view is attested, meaning, memberships in system entitlements (`UNSAccountInUNSGroup`) and the content of the snapshot is restricted to **Object references: related objects 1-3 only** by the attestation procedure, then the snapshot in the attestation procedure contains only the proxy object (`UNSAccount`). Other properties of the associated base object (for example, `AADUser`) are not displayed.	37035
If the **QER | Attestation | ReuseDecision** configuration parameter is set, approval granted by a previous approval step is not accepted if an intermediate approval step was denied approval.	37051
The compliance check in the shopping cart causes a rule violation for a subidentity although the subidentity did not break the rule.	37079
Calculation tasks are set for the compliance check when identities are added if the rule condition applies to all identities.	37097
Error importing enabled company policies with the Database Transporter. Error message: `QERPolicy: Write permission denied for value "IsWorkingCopy"`.	37098
When calculating the risk index for an object, **#** is entered as **Changed by** (`XUserUpdated`).	37130
Incorrect sort order in the **Request History** report in the Manager.	37135
Error in the formatting script for `AOBApplication.NextRunDate` when determining a valid date value.	37150, 431402

Resolved issue	Issue ID
Typo in the German version of the **IT Shop request - expires** mail template.	37221

See also:

- Schema changes on page 49
- Patches for synchronization projects on page 57

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

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, 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.	27793
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.	29535

Known Issue	Issue ID
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.	
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 the server 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 detailed information about displaying dates and time, see the *One Identity Manager Configuration Guide*.	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

Table 13: 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	32364

Known Issue	Issue ID
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.	
It is not possible to use the Web Designer to place a link in the header of the Web Portal next to the company name/logo.	32830
In the Web Portal, it is possible to subscribe to a report without selecting a schedule. Workaround: • Create an extension to the respective form, which displays a text message under the menu explaining the problem. • Add a default schedule to the subscribable report. • In the Web Designer, change the **Filter for subscribable reports** configuration key (**VI_Reporting_Subscription_Filter-RPSSubscription**) and set the schedule's **Minimum character count** value (`UID_DialogSchedule`) to **1**.	32938

If the application is supplemented with custom DLL files, an incorrect version of the `Newtonsoft.Json.dll` file might be loaded. This can cause the following error when running the application:
`System.InvalidOperationException: Method may only be called on a Type for which Type.IsGenericParameter is true.`
`at System.RuntimeType.get_DeclaringMethod()`
There are two possible solutions to the problem:
• The custom DLLs are compiled against the same version of the `Newtonsoft.Json.dll` to resolve the version conflict.
• Define a rerouting of the assembly in the corresponding configuration file (for example, `web.config`).
Example:
`<assemblyBinding >`
`<dependentAssembly>`
`<assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30AD4FE6B2A6AEED" culture="neutral"/>`
`<bindingRedirect oldVersion="0.0.0.0-11.0.0.0" newVersion="11.0.0.0"/>`
	33867

Known Issue	Issue ID
`</dependentAssembly>` `</assemblyBinding>`	
In the Web Portal, the details pane of a pending attestation case does not show the expected fields if the default attestation procedure is not used, but a copy of it is. Solution: • The object-dependent references of the default attestation procedure must also be adopted for the custom attestation procedure.	34110

Table 14: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows 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 primary SIP addresses are stored until now.	27042
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.`	29253

Known Issue	Issue ID
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 user account. - OR - • A company is assigned to the central system.	
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
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
Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping 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`.	31017
If a SharePoint site collection only has read access, the server farm account cannot read the schema properties `Owner`, `SecondaryContact`, and `UserCodeEnabled`.	31904

Known Issue	Issue ID
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.	

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 .Net Connector 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, add the following settings to `StdioProcessor.exe.config`.
• In the existing `<configSections>`:
`<sectionGroup name="SAP.Middleware.Connector">`
`<section name="GeneralSettings" type="SAP.Middleware.Connector.RfcGeneralConfiguration, sapnco, Version=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c7f7d23" />`
`</sectionGroup>`
• A new section:
`<SAP.Middleware.Connector>`
`<GeneralSettings anyDateTimeValueAllowed="true" />`
`</SAP.Middleware.Connector>`
	32149

There are no error messages in the file that is generated in the `PowershellComponentNet4` process component, in `OutputFile` parameter. Cause: No messages are collected in the file (parameter `OutputFile`). The file serves as an export file for objects returned in the pipeline. Solution: Messages in the script can be outputted using the *> operator to a file specified in the script. Example: `Write-Warning "I am a message" *> "messages.txt"` Furthermore, messages that are generated using `Write-Warning` are also	32945

Known Issue	Issue ID
written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an `Exception`. This message then appears in the One Identity Manager Service's log file.	
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 *One Identity Manager Administration Guide for Connecting to Google Workspace*.	33104
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
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
The process of provisioning object changes starts before the synchronization project has been updated. Solution: Reactivate the process for provisioning object changes after the `DPR_Migrate_Shell` process has been processed.	34903
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.	37116

Known Issue	Issue ID

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 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'`	

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. Possible cause: The number of processes started has reached the limit configured on the server.	27830
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
Valid CSS code causes an error under Mono if duplicate keys are used. For more information, see https://github.com/mono/mono/issues/7455.	762534, 762548, 29607
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 • Windows Server 2008 R2: KB4462926 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
When connecting an external web service using the web service integration wizard, the web service supplies the data in a `WSDL` file. This data is converted into Visual Basic .NET code with the Microsoft WSDL tools. If, in code generated in this way, default data types are overwritten (for example, if the `boolean` data type is redefined), it can lead to various problems in One Identity Manager.	31998
In certain Active Directory/Microsoft Exchange topologies, the `Set-Mailbox`	33026

Known Issue	Issue ID

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 Windows PowerShell call.	

Schema changes

The following provides an overview of schema changes from version 9.1.1 up to version 9.2.

Configuration Module

- New column `DialogParameter.QueryDisplayType` for displaying data in value queries.
- New column `DialogTable.IsApiServerEnabled` (in preparation for future functionality).
- New columns `DialogTree.InitScript` and `DialogTree.ListTitle` for context-sensitive displaying of display texts in the user interface.
- New column `QBMHtmlApp.UID_QBMDBPrincipal` for mapping the minimum access level for using HTML applications.
- New column `DialogDeferredOperation.XObjectKey`.
- New columns `QBMNonLinearDepend.XUserInserted`, `QBMNonLinearDepend.XUserUpdated`, `QBMNonLinearDepend.XDateInserted`, and `QBMNonLinearDepend.XDateUpdated`.
- New tables `QBMConfigLibrary` and `QBMConfigLibraryCategory` for providing a configuration library of templates and formatting rules.

- New table `QBMMissingDisplayRight` for quickly determining display permissions.
- New table `QBMUserConfig` for the internal mapping of user settings.

Target System Synchronization Module

- New column `DPRProjectionConfig.GeneralConcurrenceStrategy` for specifying a strategy to detect collisions.
- New columns `DPRProjectionStartInfo.FailureHandlingMode` and `DPRProjectionStartInfo.FailureHandlingRetryCycles` for improved handling of failed objects.
- New columns `DPRProjectionStartInfo.SysConcurrenceCacheLifeTime` and `DPRProjectionStartInfo.SysConcurrenceCheckMode` for improved detection of processing conflicts.
- New columns `DPRSchemaProperty.IsMvpOrderSignificant` and `DPRSystemMappingRule.MvpOrderBehavior` for handling MVP values when detecting rogue modifications.

Target System Base Module

- New columns `TSBVAccountTable.ColumnNameAccDisabled` and `TSBVAccountTable.IsPersonAuto4Disabled` to improve mapping user accounts of locked identities.
- The columns `TSBVUNSDomain.AlternatePropertyCaptions`, `TSBVUNSRoot.AlternatePropertyCaptions`, and `UNSRoot.AlternatePropertyCaptions` have been deleted.

Azure Active Directory Module

- New column `AADAdministrativeUnit.UID_AERoleOwner` for mapping owners of administrative units.
- New column `AADApplication.UID_AERoleOwner` for mapping application owners.
- New column `AADServicePrincipal.UID_AERoleOwner` for mapping service principal owners.
- New columns for supporting other Identity Management relevant property of user accounts.
    - `AADUser.EmployeeHireDate`
    - `AADUser.EmployeeLeaveDateTime`
    - `AADUser.EmployeeType`
    - `AADUser.EodCostCenter`
    - `AADUser.EodDivision`
- New columns for determining user account login times.

    - AADUser.siaLastNISignInDateTime
    - AADUser.siaLastNISignInRequestId
    - AADUser.siaLastSignInDateTime
    - AADUser.siaLastSignInRequestId
- New column AADOrganization.RoleBehavior for mapping Azure Active Directory role management.
- New tables for mapping Azure Active Directory role management.
    - AADBaseTreeHasScopedRLAsgn
    - AADBaseTreeHasScopedRLElgb
    - AADGroupInScopedRLAsgn
    - AADGroupInScopedRLElgb
    - AADPrincipalInScopedRLAsgn
    - AADPrincipalInScopedRLElgb
    - AADRole
    - AADRoleAssignment
    - AADRoleEligibility
    - AADRoleManagementPolicy
    - AADScopedRLAsgn
    - AADScopedRLElgb
    - AADUserInScopedRLAsgn
    - AADUserInScopedRLElgb
    - DepartmentHasScopedRLAsgn
    - DepartmentHasScopedRLElgb
    - LocalityHasScopedRLAsgn
    - LocalityHasScopedRLElgb
    - OrgHasScopedRLAsgn
    - OrgHasScopedRLElgb
    - ProfitCenterHasScopedRLAsgn
    - ProfitCenterHasScopedRLElgb

Exchange Online Module

- New columns for mapping hierarchical address books.
    - AADOrganization.UID_O3EDLHABRoot
    - O3EDL.IsHierarchicalGroup
    - O3EDL.PhoneticDisplayName

- O3EDL.SeniorityIndex
- O3EMailbox.PhoneticDisplayName
- O3EMailbox.SeniorityIndex

Microsoft Teams Module

- New column O3TTeam.tmsAllowCreatePrivateChannels for specifying whether members can create or update private channels.
- New table O3TTeamTemplate and new column O3TTeam.UID_O3TTeamTemplate for mapping Teams templates.

Active Directory Module

- New columns for supporting POSIX properties of user accounts, contacts, and groups.
  - ADSAccount.Gecos
  - ADSAccount.GidNumber
  - ADSAccount.LoginShell
  - ADSAccount.UidNumber
  - ADSAccount.UidPosix
  - ADSAccount.UnixHomeDirectory
  - ADSContact.Gecos
  - ADSContact.GidNumber
  - ADSContact.LoginShell
  - ADSContact.UidNumber
  - ADSContact.UidPosix
  - ADSContact.UnixHomeDirectory
  - ADSGroup.GidNumber

Microsoft Exchange Module

- New columns for mapping hierarchical address books.
  - EX0DL.IsHierarchicalGroup
  - EX0DL.PhoneticDisplayName
  - EX0DL.SeniorityIndex
  - EX0MailBox.PhoneticDisplayName
  - EX0MailBox.SeniorityIndex
  - EX0MailContact.PhoneticDisplayName
  - EX0MailContact.SeniorityIndex

    - EX0MailUser.PhoneticDisplayName
    - EX0MailUser.SeniorityIndex
    - EX0Organization.UID_EX0DLHABRoot
- New table EX0VHABMembers for mapping hierarchical address books.
- New table EX0DLSendAsPerm for mapping send permissions of mail-enabled distribution groups.

Exchange Hybrid Module

- New columns EXHRemoteMailbox.PhoneticDisplayName and EXHRemoteMailbox.SeniorityIndex for mapping hierarchical address books.

LDAP Module

- New columns for supporting the eduPerson object class.
    - LDAPAccount.EduPersonAffiliation
    - LDAPAccount.EduPersonAnalyticsTag
    - LDAPAccount.EduPersonAssurance
    - LDAPAccount.EduPersonEntitlement
    - LDAPAccount.EduPersonNickname
    - LDAPAccount.EduPersonOrcId
    - LDAPAccount.EduPersonOrgDN
    - LDAPAccount.EduPersonOrgUnitDN
    - LDAPAccount.EduPersonPrimaryAffiliation
    - LDAPAccount.EduPersonPrimaryOrgUnitDN
    - LDAPAccount.EduPersonPrincipalName
    - LDAPAccount.EduPersonPrincipalNamePrior
    - LDAPAccount.EduPersonScopedAffiliation
    - LDAPAccount.EduPersonTargetedId
    - LDAPAccount.EduPersonUniqueId

Domino Module

- New columns for supporting Notes roaming user accounts.
    - NDOUser.RoamAB
    - NDOUser.RoamCleanPer
    - NDOUser.RoamCleanSetting
    - NDOUser.RoamExtFiles
    - NDOUser.RoamingUser

- NDOUser.RoamMode
- NDOUser.RoamSubDir
- NDOUser.UID_NDOServerRoamSrvr

OneLogin Module

- New column OLGUser.AccountDisabled for specifying whether the user account is locked.

Privileged Account Governance Module

- New tables PAGPartition and PAGPartitionIsManagedBy for mapping partitions.
- New columns PAGAsset.UID_PAGPartition and PAGDirectory.UID_PAGPartition for mapping partitions.
- New columns for supporting access requests for API keys.
  - PAGAstAccount.AllowApiKeyRequest
  - PAGAstAccount.HasApiKeys
  - PAGAstAccount.HasTotpAuthenticator
  - PAGAstAccount.IsApplicationAccount
  - PAGUserAttestation.AllowApiKeyRequest
- New columns PAGReqPolicy.LinkedAccountScopeFiltering and PAGReqPolicy.UseAltLoginName for PAM access request policies.
- New column PAGEntl.XDateSubItem for mapping the change date of dependent objects.
- New table PAGAuditLog for mapping audit logs to support Behavior Driven Governance.

Unix Based Target Systems Module

- New columns for mapping user account login data.
  - UNXAccount.LastLogin
  - UNXAccount.LastLoginString
  - UNXAccount.LastPasswordChange
  - UNXHost.UID_DialogTimeZone

Identity Management Base Module

- New column Person.LeaveOfAbsenceReason as reason for absence of an identity.
- New column QERTermsOfUse.IsAcceptRequiresMfa for specifying whether multifactor authentication is required to accept the terms of use.

Company Policies Module

- New columns `QERPolicy.IsToAttestImmediately` and `QERPolicy.ObjectKeyAttPolicy` to support automatic attestation of policy violations.

Attestation Module

- New column `AttestationPolicy.IsNoRunOnEmptyResult` to specify whether an empty attestation run is generated when no attestation object was found.

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 9.1.1 up to version 9.2. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 82.

Modified synchronization templates

The following provides you with an overview of modified synchronization templates. Patches are made available for updating synchronization templates in existing synchronization projects. For more information, see Patches for synchronization projects on page 57.

Table 17: Overview of synchronization templates and patches

Module	Synchronization template	Type of modification
Target System Synchronization Module	Automatic One Identity Manager synchronization	changed
Azure Active Directory Module	Azure Active Directory synchronization	changed
	Azure Active Directory B2C tenant	changed
Active Directory Module	Active Directory synchronization	changed
Active Roles Module	Synchronize Active Directory domain via Active Roles	changed
Cloud Systems Management Module	Universal Cloud Interface	none

Module	Synchronization template	Type of modification
	synchronization	
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	none
	Oracle E-Business Suite CRM data	none
	Oracle E-Business Suite HR data	none
	Oracle E-Business Suite OIM data	None
Microsoft Exchange Module	Microsoft Exchange 2013/2016/2019 synchronization (v2)	changed
Google Workspace Module	Google Workspace synchronization	none
LDAP Module	AD LDS synchronization	None
	AD LDS Synchronization (version 2)	None
	OpenDJ synchronization	None
	OpenDJ Synchronization (version 2)	None
	Generic LDAP Synchronization (version 2)	None
	Oracle DSEE Synchronization (version 2)	None
Domino Module	Lotus Domino Synchronization	changed
Exchange Online Module	Exchange Online synchronization (v2)	None
Microsoft Teams Module	Microsoft Teams (via Azure Active Directory)	None
OneLogin Module	OneLogin Domain Synchronization	None
Privileged Account Governance Module	One Identity Safeguard synchronization	changed
SAP R/3 User Management Module	SAP R/3 synchronization (Base	changed

Module	Synchronization template	Type of modification
	Administration)	
	SAP R/3 (CUA subsystem)	none
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	none
SAP R/3 Compliance Add-on Module	SAP R/3 authorization objects	none
SAP R/3 Structural Profiles Add-on Module	SAP R/3 HCM authentication objects	none
	SAP R/3 HCM employee objects	none
SharePoint Module	SharePoint synchronization	none
SharePoint Online Module	SharePoint Online synchronization	none
Universal Cloud Interface Module	SCIM Connect via One Identity Starling Connect	changed
	SCIM synchronization	changed
	SCIM synchronization of an SAP Cloud ALM application	new
Unix Based Target Systems Module	Unix Account Management	changed
	AIX Account Management	changed

Patches for synchronization projects

Patches for the following patch types are provided in One Identity Manager 9.2.

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

To adjust existing synchronization projects to One Identity Manager version 9.2, 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 9.2.

Patches for new features can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 9.2 for synchronization projects. Only the patches that were newly created after version 9.1.1 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 on page 82.

Table 18: General patches

Patch ID	Patch	Description	Issue ID
VPR#36755	Disables the synchronization buffer for the central database	Disables the synchronization buffer for various virtual schema properties in the central database schema in synchronization projects for system synchronization.	36755
	Milestone 9.2	Milestone for the context **DPR**.	
	Milestone 9.2	Milestone for the context **One Identity Manager**.	

Table 19: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#36596	Support for connection certificates	Adds the `CP_CertificateThumbprint` variable to the default variable set. This patch is applied automatically when One Identity Manager is updated.	36596
VPR#36729	New schema property for Azure Active Directory user account	Adds property mapping rules for the `employeeHireDate`, `employeeLeaveDateTime`, `employeeType`, `eoddivision`, and `eodcostcenter` schema properties to the `User` mapping. This patch is applied automatically when One Identity Manager is updated.	36729
VPR#36799	Sets filters in multi-reference rules	Inserts member filters in various multi-reference rules for the `Owners` schema property. This patch is applied automatically when One Identity Manager is updated.	36799

Patch ID	Patch	Description	Issue ID
VPR#33776	New schema properties for mapping the login times of Azure Active Directory user accounts	Adds property mapping rules for mapping the last login times of user accounts (`siaLastNISignInDateTime`, `siaLastNISignInRequestId`, `siaLastSignInDateTime`, `siaLastSignInRequestId`) to the `User` mapping. These schema properties can only be accessed under an Azure Active Directory premium license.	33776
VPR#35769	Enables service principals to be mapped as service principal owners	Extends the member filter of the `vrtOwners_Owners` property matching rule in the `ServicePrincipal` mapping to include service principals. This patch is applied automatically when One Identity Manager is updated.	35769
VPR#35513	Support for RBAC and PIM features	Extends the synchronization configuration to synchronize objects for role-based access control (RBAC) and privileged identity management (PIM). This patch is applied automatically when One Identity Manager is updated.	35513
	Milestone 9.2	Milestone for the context **Azure Active Directory**.	

Table 20: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#14634	New maps for mapping POSIX properties	Adds the `posixUser`, `posixGroup`, and `posixContact` mappings for mapping POSIX properties of user accounts, groups, and contacts.	14634
	Milestone 9.2	Milestone for the context **Active Directory**.	

Table 21: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#14634_ ARS	New property mapping rules for POSIX properties	Adds property mapping rules to the `User`, `InetOrgPerson`, `Group`, and `Contact` mappings to map POSIX properties.	14634
	Milestone 9.2	Milestone for the context **Active Roles**.	

Table 22: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#35776	Extends send as permissions	Extends the synchronization configuration to support send-as permissions for distribution groups. This patch is applied automatically when One Identity Manager is updated.	35776
VPR#35779	New property mapping rules for mapping a hierarchical address book	Adds to property mapping rules to various mapping to map a hierarchical address book. This patch is applied automatically when One Identity Manager is updated.	35779
	Milestone 9.2	Milestone for the context **Microsoft Exchange**.	

Table 23: Patches for HCL Domino

Patch ID	Patch	Description	Issue ID
VPR#36087	Mapping of user account roaming properties	Extends the `Person` mapping to map user account roaming properties. This patch is applied automatically when One Identity Manager is updated.	36087
VPR#36831	Remove quotas for deleting objects	Removes quotas for the `Delete object` method from the `CertifierRequest` and `AdminRequest` synchronization steps.	36831
	Milestone 9.2	Milestone for the context **HCL Domino**.	

Table 24: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#35780	New property mapping rules for mapping a hierarchical address book	Adds to property mapping rules to various mapping to map a hierarchical address book. This patch is applied automatically when One Identity Manager is updated.	35780
	Milestone 9.2	Milestone for the context **Exchange Online**.	

Table 25: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#36961	Removes unused schema properties	Removes unused virtual schema properties from the `Web` schema type.	36961
	Milestone 9.2	Milestone for the context **SharePoint Online**.	

Table 26: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#36044	Support for One Identity Safeguard partitions	Extends the synchronization configuration to support One Identity Safeguard partitions.	36044
VPR#36315	Maps the One Identity Safeguard audit log	Extends the synchronization configuration to load the One Identity Safeguard audit log (`AuditLog`).	36315
VPR#36617	Support for One Identity Safeguard 7.2 and 7.3	Extends the synchronization configuration to support One Identity Safeguard versions 7.2 and 7.3	36617, 36943
	Milestone 9.2	Milestone for the context **Privileged Account Management**.	

Table 27: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#36970	Sets reload threshold of user accounts	Sets the reload threshold in the `user` synchronization step to the value **4**.	36970
	Milestone 9.2	Milestone for the context **SAP R/3**.	

Table 28: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
VPR#35904	Removes unused processing methods	Remove unused processing methods (`Update`) in different synchronization steps.	35904
	Milestone 9.2	Milestone for the context **SAP R/3**.	

Table 29: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#36376	New variable for configuring list settings	Adds a variable for configuring the number of elements per page when requested for the objects list in the default variable set and the connection parameters. This patch is applied automatically when One Identity Manager is updated.	36376
VPR#36985	Schema extension corrections	Saves the name of the schema type extensions in the schema. This patch is applied automatically when One Identity Manager is updated.	36985
	Milestone 9.2	Milestone for the context **SCIM**.	

Table 30: Patches for Unix

Patch ID	Patch	Description	Issue ID
VPR#36688	New property mapping rules for mapping the last login times and last password changes of user accounts	Adds property mapping rules for `LastPasswordChange` and `LastLogin` to the `User` mapping. This patch is applied automatically when One Identity Manager is	36688

Patch ID	Patch	Description	Issue ID
		updated.	
	Milestone 9.2	Milestone for the context **Unix**.	

Deprecated features

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

- The following scripts have been removed:
  - VI_GetValueOfObject
  - VID_GetValueOfDialogObject
  - VI_ITDataFromOrg
  - VI_AE_ITDataFromOrg
  - VI_GetOrgUnitFromCertifier
  - VI_ConvertDNToCanonicalName
  - VI_PersonAuto_LDAP
  - VI_PersonAuto_ADS
  - VI_PersonAuto_EBS
  - VI_PersonAuto_Notes
  - VI_PersonAuto_SAP
  - VI_PersonAuto_SharePoint_SPSUser
  - VI_GetAttestationObject
  - VI_GetDNParser
  - TSB_Find_And_Use_Linked_Account_For_AccountDef
- The following configuration parameters have been removed.
  - TargetSystem | ADS | DBDeleteOnError
  - TargetSystem | ADS | VerifyUpdates
  - TargetSystem | EBS | DBDeleteOnError
  - TargetSystem | NDO | VerifyUpdates
  - TargetSystem | SAPR3 | DBDeleteOnError
  - TargetSystem | SAPR3 | VerifyUpdates
  - TargetSystem | SharePoint | DBDeleteOnError

The following features will be discontinued in future versions of One Identity Manager and should no longer be utilized:

- The following features will not be supported in the One Identity Manager Service in future.
  - FileJobProvider
  - FileJobDestination
  - FileJobGate
  - FTPJobProvider
  - FTPJobDestination
  - HTTPJobProvider
  - HTTPJobDestination
  - HTTPJobGate
- The Web Designer and Web Designer-based web applications will not be supported in future. Use the HTML web applications that are provided via the API Server.
- The `PersonPasswordHistory` table will be removed in future versions.
- The following scripts are labeled obsolete. A warning to this effect is issued during compilation.
  - VI_AE_BuildCentralAccount
  - VI_AE_BuildCentralAccountGlobalUnique
  - VI_BuildInternalName
  - VI_AE_CreatedefaultMailAddress
  - VI_AE_BuildCentralSAPAccount

System requirements

Before installing One Identity Manager 9.2, ensure that your system meets the following minimum hardware and software requirements.

For more detailed information about system prerequisites, see the *One Identity Manager Installation Guide*.

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 requirements for using SQL Server as a database server

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.

Processor	8 physical cores with 2.5 GHz+ frequency (non-production) 16 physical cores with 2.5 GHz+ frequency (production) 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 2019 Standard Edition (64-bit) with the latest cumulative update • 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.

- Compatibility level for databases: SQL Server 2019 (150)
- 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

To run the One Identity Manager database in a managed instance in Azure SQL Database, you require the **Business critical** tier. For more information, see the Microsoft site under https://azure.microsoft.com/en-us/products/azure-sql/database/.

Minimum requirements for clients

The following system requirements must be met on the clients.

Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	1 GB
Operating system	Windows operating systems

	Following versions are supported: • Windows 11 (x64) • Windows 10 (32-bit or 64-bit) with version 1511 or later
Additional software	• Microsoft .NET Framework version 4.8 or later • Microsoft Edge WebView2
Supported browsers	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimum requirements for the Job server

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

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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project.
Additional software	Windows operating systems • Microsoft .NET Framework version 4.8 or later NOTE: Take the target system manufacturer's recommendations for connecting the target system into account. Linux operating systems • Mono 6.10 or later

Minimum requirements for the web server

The following system prerequisites must be fulfilled to install web applications on a web server.

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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.

Additional software	Windows operating systems
	• Microsoft .NET Framework version 4.8 or later
	• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.8 and the Role Services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • Web Server > Application Development > ASP.NET
	  • Web Server > Application Development > .NET Extensibility
	  • Web Server > Application Development > ISAPI Extensions
	  • Web Server > Application Development > ISAPI Filters
	  • Web Server > Security > Basic Authentication
	  • Web Server > Security > Windows Authentication
	  • Web Server > Performance > Static Content Compression
	  • Web Server > Performance > Dynamic Content Compression

	Linux operating system
	• NTP - Client
	• Mono 6.10 or later
	• Apache HTTP Server 2.0 or 2.2 with the following modules:
	  • mod_mono
	  • rewrite
	  • ssl (optional)

Minimum requirements for the application server

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

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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.
Additional software	Windows operating systems • Microsoft .NET Framework version 4.8 or later • Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.8 and the Role Services:

- Web Server > Common HTTP Features > Static Content
- Web Server > Common HTTP Features > Default Document
- Web Server > Application Development > ASP.NET
- Web Server > Application Development > .NET Extensibility
- Web Server > Application Development > ISAPI Extensions
- Web Server > Application Development > ISAPI Filters
- Web Server > Security > Basic Authentication
- Web Server > Security > Windows Authentication
- Web Server > Performance > Static Content Compression
- Web Server > Performance > Dynamic Content Compression

Linux operating system

- NTP - Client
- Mono 6.10 or later
- Apache HTTP Server 2.0 or 2.2 with the following modules:
  - mod_mono
  - rewrite
  - ssl (optional)

Supported data systems

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

Table 31: 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

Connector	Supported data systems
	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.
Web service connector	Any SOAP web service providing wsdl. NOTE: You can use the web service wizard to generate the configuration to write data to the web service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active Directory connector	Active Directory shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 and Windows Server 2022.
Microsoft Exchange connector	• Microsoft Exchange 2013 with cumulative update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange Hybrid environments
SharePoint connector	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
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, 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)
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the specifications for One Identity Authentication Services.
Domino connector	• IBM Domino Server versions 8, 9, and 10 • HCL Domino Server versions 11 and 12 • IBM Notes Client 8.5.3 and 10.0 • HCL Notes Client versions 11.0.1 and 12.0

Connector	Supported data systems
	The 64-bit variant of Notes Client 12.0.1 is currently not supported. 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) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe connector	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.5, 7.5.2, 7.5.3, 7.6, 8.0, 8.1.1, and 8.1.3
Azure Active Directory connector	• Microsoft Azure Active Directory NOTE: Synchronization of Azure Active Directory tenants in national cloud deployments with the Azure Active Directory connector is not supported. This affects: • Microsoft Cloud for US Government (L5) • Microsoft Cloud Germany • Azure Active Directory and Microsoft 365 operated by 21Vianet in China 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

Connector	Supported data systems
	2.0. They must conform to RCF 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
Google Workspace connector	• Google Workspace
Oracle E-Business Suite connector	• Oracle E-Business Suite versions 12.1, 12.2, and 12.2.10
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard versions 6.0, 6.7, 6.13, 7.0, 7.1, 7.2, and 7.3 You can find the Windows 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 Windows 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 initial One Identity Manager LTS release is 9.0. For all LTS releases of One Identity Manager, the first digit identifies the release and the second is always a zero (for example, 9.0).
- Maintenance LTS Releases (known as Cumulative Updates): A third digit is added; for example, 9.0.1.

Feature Release

- Feature Releases' version numbers are two digits (for example, 9.1, 9.2, etc).

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

Table 32: Comparison of Long Term Support (LTS) Release and Feature Release

Category	Long Term Support (LTS) Release	Feature Release
Release frequency	Every 36 months (includes resolved issues and security related updates).	Approximately every 12 months (includes resolved issues and security related updates).
Duration of full support	36 months	18 months
Duration of limited support	12 months (after the end of full support)	6 months (after the end of full support)
Versioning	All versions where the second number is **0**. For example: 9.0.0 (9.0.1, 9.0.2,), 10.0.0, 11.0.0, and so on.	All versions where the second number is not **0**. For example: 9.1.0 (9.1.1, 9.1.2), 9.2, 9.3, 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, 9.0 LTS) by installing a later feature release or version (for example 9.2). Once this has happened, you are not on the LTS

support path until the next LTS base version (10.0, 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 9.2 to 9.0 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 10.0 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 to see 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 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 want currently use version 9.1.1 and want to upgrade to 9.2, and, for example, versions 9.1.3, 9.1.4, and 9.1.5 have been released, you only have to install version 9.2 and it automatically applies the resolved issues from 9.1.3, 9.1.4, and 9.1.5.

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 9.0, 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 9.0 (LTS) and decide to move to 9.2, you will come off the LTS support path until you install the next base LTS version (10.0, 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.

Upgrade and installation instructions

To install One Identity Manager 9.2 for the first time, follow the installation instructions in the *One Identity Manager Installation Guide*. For detailed instructions about updating, see the *One Identity Manager Installation Guide*.

IMPORTANT: Note the Advice for updating One Identity Manager on page 76.

Advice for 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 9.2. 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 version 8.0.x to version 9.2, 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>';
  column 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 about archiving data, see the *One Identity Manager Data Archiving Administration Guide*.
- 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.
- During installation of a new One Identity Manager database with version 9.2 or while updating a One Identity Manager database from version 8.0.x to version 9.2, you can specify whether you want to work with granular permissions at server and database level. The Configuration Wizard then creates SQL Server logins and database users

with the necessary permissions for administrative user, configuration users and end users. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

After updating One Identity Manager, change the connection parameters. This affects, for example, the connection data for the database (`DialogDatabase`), the One Identity Manager Service, the application server, the administration and configuration tools, the web applications and web services as well as the connection data in synchronization projects.

> NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.2, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.
>
> If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

- 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. For more information, see the *One Identity Manager Authorization and Authentication Guide*.

Updating One Identity Manager to version 9.2

> IMPORTANT: Note the Advice for updating One Identity Manager on page 76.

To update an existing One Identity Manager installation to version 9.2

1. Run all the consistency checks in the Designer in **Database** section.
   a. Start the Consistency Editor in the Designer by selecting the **Database > Check data consistency** menu item.
   b. In the **Test options** dialog, click  .
   c. Under the **Database** node, enable all the tests and click **OK**.
   d. Select the **Consistency check > Run** menu item to start testing.

      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.

a. Run the program `autorun.exe` from the root directory on the One Identity Manager installation medium.

b. Change to the **Installation** tab. Select the Edition you have installed.

c. Click **Install**.

   This starts the installation wizard.

d. 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. Check whether the database's compatibility level is set the **150** and change it if necessary.
6. 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.

     NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.2, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

     If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.
7. Update the One Identity Manager Service on the update server.

   a. Run the `autorun.exe` program from the root directory on the One Identity Manager installation medium.

   b. Change to the **Installation** tab. Select the Edition you have installed.

   c. Click **Install**.

      This starts the installation wizard.

   d. 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.

8. Check the login information of the One Identity Manager Service. Specify the service account to use.
9. Start the One Identity Manager Service on the update server.
10. 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 9.2

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 project 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 `DPR_Migrate_Shell` process 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 on page 82.

To update an application server to version 9.2

- After updating the One Identity Manager database's schema, the application server starts the automatic 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 the Web Designer Web Portal to version 9.2

NOTE: Ensure that the application server is updated before you update the Web Designer Web Portal.

- To update the Web Designer Web Portal automatically, connect to the runtime monitor http://<server>/<application>/monitor in a browser and start the web application update.
- To manually update the Web Designer Web Portal, uninstall the existing Web Designer Web Portal installation and reinstall the Web Designer Web Portal. For more instructions, see the *One Identity Manager Installation Guide*.

To update an API Server to version 9.2

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

To update the Operations Support Web Portal to version 9.2

- (As from version 8.1.x) After updating the API Server, the Operations Support Web Portal is also current.
- (As from version 8.0.x)
    1. Uninstall the Operations Support Web Portal.
    2. Install an API Server. For more instructions, see the *One Identity Manager Installation Guide*.

To apply changes from version 9.2 to your HTML applications

1. Load the current source code from the One Identity Github repository.
2. Pull the changes from the **v92** branch into your repository.
3. Compile your HTML application and fix any compilation errors that may occur.

   For more information, see the *One Identity Manager HTML5 Development Guide*.
4. Check whether you HTML application still work properly.
5. Deploy the new version of your HTML application.

   For more information, see the *One Identity Manager HTML5 Development Guide*.

To update the Manager web application to version 9.2

1. Uninstall the Manager web application
2. Reinstall the Manager web application.
3. The Internet Information Services default user requires write permissions to the Manager web application installation directory so that Manager web applications can be updated automatically. Check that the correct permissions are allocated.

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 application 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 customization 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 the *One Identity Manager Target System Synchronization Reference Guide*.

See also:

- Modified synchronization templates on page 55
- Patches for synchronization projects on page 57

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 2023.0009.0002.0000 for all modules and the application version 9.2 v92-226554 indicate that this version is installed.

Additional resources

Additional information is available from the following:

- One Identity Manager Support
- One Identity Manager Online documentation
- One Identity Manager Community
- One Identity Manager Training portal website

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.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product