

One Identity Manager 8.1

Release Notes

March 2019

These release notes provide information about the One Identity Manager release, version 8.1. You will find all the modifications since One Identity Manager version 8.0.2 listed here.

One Identity Manager 8.1 is a minor release with new functionality and improved behavior. See [New features](#) on page 2 and [Enhancements](#) on page 8.

If you update a One Identity Manager version that is older than One Identity Manager 8.0.2, read the release notes from the previous versions as well. You can find the release notes under [One Identity Manager Support](#).

For information about changes in the Data Governance Edition, see the *One Identity Manager Data Governance Edition Release Notes*.

For information about changes in the ServiceNow module, see the *One Identity Manager and ServiceNow Integration Release Notes*.

For information about changes in the Cloud HR System module, see the *One Identity Manager and Cloud HR Systems Integration Release Notes*.

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 8.1

One Identity Manager simplifies the process of managing user identities, access permissions and security policies. You allow the company control over identity management and access decisions whilst the IT team can focus on their core competence.

With this product, you can:

- Implement group management using self-service and attestation for Active Directory with the One Identity Manager Active Directory Edition
- Realize Access Governance demands cross-platform within your entire concern with One Identity Manager

Each one of these scenario specific products is based on an automation-optimized architecture that addresses major identity and access management challenges at a fraction of the complexity, time, or expense of "traditional" solutions.

One Identity Hybrid Subscription

The newest version of our on-prem products will offer a mandatory One Identity Hybrid Subscription, which helps our customer's transition to a hybrid environment on their way to the cloud. The subscription enables you to join their on-prem solutions with our One Identity Starling software-as-a-service platform. Giving your organization immediate access to a number of cloud-delivered features and services, which expand the capabilities of your on-prem product. We will continuously make available new products and features to our One Identity SaaS platform. With the One Identity Hybrid Subscription, you can use these immediately for their One Identity on-prem solutions and their subscription continues to add value.

Expand the capabilities of One Identity Manager with [One Identity Hybrid Subscription](#), which offers a myriad of additional cloud-delivered features and services. Gain access to all-you-can-eat [Starling Two-Factor Authentication](#) to protect administrative access, to enforce additional factor authentication when requesting or approving critical access or to enable out of band user verification for password requests. For an additional cost, these offerings can also be extended to additional target systems and use cases. A single subscription can be used for all your One Identity products.

New features

New features in One Identity Manager 8.1:

Basic functionality

- For information about the minimum system prerequisites, see [System requirements](#) on page [61](#).
- Oracle Database is no longer supported as a database system for the One Identity

Manager database.

- One Identity Manager uses In-Memory OLTP ((Online Transactional Processing) for memory optimized data access. The database server must support Extreme Transaction Processing (XTP). Take the [Advice for updating One Identity Manager](#) on page 69 into account at the same time.

- Support for granular permissions at server and data level.

SQL Server logins and database users are provided with the necessary permissions for administrative users, configuration users and end users. Take the [Advice for updating One Identity Manager](#) on page 69 into account at the same time. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

Some front-ends expect a minimum of configuration level user permissions. In this case, end user login is not supported. The permissions level for the current user is also shown in the login dialog.

- The front-ends check whether the user has the required permissions before starting up. Users can only start up front-ends if they own permissions groups for the corresponding program functions. For more detailed information, see the *One Identity Manager Authorization and Authentication Guide*.
- Role based permissions groups can be assigned to an application. In this case, the permissions of the permissions group only apply for this application. When a user logs on to the application, they receive the permissions of the permissions group in addition to their own permissions.
- One Identity Manager logoffs can be written to the system journal. To enable this, set the configuration parameter **Common | Journal | LogoffAudit**. Logins and logoffs are available for analysis in the QBM_VDialogJournalLoginAudit view.
- Improved support for troubleshooting
 - Object Browser supports debugging of scripts, templates, format scripts, table scripts, processes and methods.

To generate local debug assemblies, enable the option **Create debug information** in Database Compiler and select the compiler setting **Scripts including all dependencies**. This option is only available for users that have obtained the program function **Allow to create local debug assemblies** (Common_CompileForDebug) through their permissions groups. The program function must be assigned to a custom permissions group.

- You can search for scripts in System Debugger. Modified scripts are marked with a *. You can save multiple scripts at the same time.
- To use System Debugger or the debug function in Object Browser, Visual Studio version 2017 with the latest Service Pack and Microsoft .NET Framework version 4.7.2 Developer Pack or later must be installed.
- Windows Step Recorder is started in the front-end's error message window and records errors in the steps.
- Support for NLog 4.5.11.

- Log displayed in the application server. The log is only visible to users that have obtained the program function **Enables log display in the application server** (AppServer_Logs) through their permissions groups.
- There is a command line program AppServer.Installer.CMD.exe available for installing an application server. You can find the program in the add-on for the Configuration Module.
- Improved OAuth 2.0/OpenID Connect configuration.

There is a wizard available in Designer for creating a OAuth 2.0/OpenID Connect configuration in One Identity Manager. Use OpenID Connect Discovery to find the configuration data or enter it manually. The data is mapped to its own tables in the One Identity Manager schema.

NOTE: During a One Identity Manager database update, existing values from configuration parameters and the web server settings are transferred to the new data structure.

The configuration parameter **QER | Person | OAuthAuthenticator** and its sub parameters have been deleted.

In Designer, check the OAuth 2.0/OpenID Connect configuration and the web server settings under **Base data | Security settings**.

- Extended support of JSON Web Key for OAuth 2.0/OpenID Connect authentication.
- There is a command line program SchemaExtensionCmd.exe available for importing schema extensions. The program requires a definition file (XML file) that can be created in the Schema Extension program. There can be several extensions given in the definition file.

With the Schema Extension program and the command line program, you can remove custom schema extensions from databases with a staging level **Test environment** or **Development system**.

- Improved support for checking passwords.
 - You can define multiple password questions and answers. The configuration parameters **QER | Person | PasswordResetAuthenticator | QueryAnswerDefinitions** and **QER | Person | PasswordResetAuthenticator | QueryAnswerRequests** control how many password questions can be defined and must be answered. The configuration parameter **QER | Person | PasswordResetAuthenticator | InvalidateUsedQuery** defines whether questions should no longer be used after the password has been reset successfully.
 - You can assign password policies to departments, cost centers, locations and business roles.
 - Password policies can be applied depending on the user account's account definition or the user account's manage level.
 - In password policies, you can specify character sets that are not permitted in generated passwords.

- The column definition specifies whether a column contains name properties to be checked in the password policy.
- An employee's central password is mapped to the employee's system user password. This behavior is defined in the configuration parameter **QER | Person | UseCentralPassword | SyncToSystemPassword**.
 - ① **NOTE:** The configuration parameter **QER | Person | UseCentralPassword | PasswordCaptureAgent | SyncSystemPassword** has been removed. The script `VI_CaptureAgent_SetPassword` has been reworked. If you overwritten the script with your own, add the changes to it.
- An employee's central password is noted in the user account passwords history and is taken into account when passwords are checked.
 - ① **NOTE:** If you have defined custom templates for password columns, check whether these should be moved to the script `QER_Publish_CentralPassword`. Overwrite the script to do this.
- By entering an employee's central password, locked system user logins, Active Directory user accounts and SAP users are unlocked. This behavior is controlled by the configuration parameters **QER | Person | UseCentralPassword | SyncToSystemPassword | UnlockByCentralPassword, TargetSystem | ADS | Accounts | UnlockByCentralPassword** and **TargetSystem | SAPR3 | Accounts | UnlockByCentralPassword**.
- Four eyes principle for issuing the passcode. The configuration parameter **QER | Person | PasswordResetAuthenticator | PasscodeSplit** controls whether passcodes generated by the help desk are divided into two parts, one for the help desk and one for the employee's manager.
- If login is employee based, customized password policies are taken into account.
- To guarantee more security, Captcha is queried with passcode, password question and password.
- Additional language settings for formatting data, such as date, time or numeric formats for users.
 - In the front-end program settings, the language for displaying text and the language for displaying values can be defined separately.
 - In the employee master data, you can specify a language for assessing values.
 - Use the configuration parameter **Common | MailNotification | DefaultCultureFormat** to specify the default language for language specific formatting of values for employees.
- Database encryption uses RSA encryption with Optimal Asymmetric Encryption Padding (OAEP). Databases that are already encrypted with a key length of > 1024 bits are not converted but continue using PKCS#1 for encryption. New encrypted values use OAEP. If you still use a key that has 1024 bits, it is recommended you

create a new key in Crypto Configuration and encrypt the database again.

- In the installation wizard, you can change the installation settings for a service if they differ from the default installation.
- The .Net Compiler Platform is used to compile the database and scripts for synchronization projects.
- In the column definitions, you can define scripts to conditionally remove the column's viewing and edit permissions.

Web applications

- With API Designer, you can quickly create, document, compile and publish a REST API. This API is based on the OpenAPI Specification and the One Identity Manager database model. The advantages of API Designer at a glance:
 - Simple and quick to use.
 - The finished API understands the One Identity Manager database model.
 - Changes to the API are transparent.
 - Supports the principles of good API design.
 - APIs that you create with help of API Designer are based, in principle, on the OpenAPI specification.

For more detailed information, see the *One Identity Manager API Designer User and Development Guide* and the *One Identity Manager HTML5 Development Guide*.

- The API Server supplies the API that you create with the help of the new API Designer.
- The Operations Support Web Portal has essentially been recreated as an HTML5 application. The underlying REST API was created with the help of the new API Designer.
- Implementation of Secure Password Extension to allow users to access the Password Reset Portal over the Windows login screen. Secure Password Extension is an application, which can access the entire functionality of the Password Reset Portal over the Windows login screen.

Secure Password Extension is an add-on for the Active Directory Module. For detailed information about configuring and distribution of Secure Password Extension, see the *One Identity Manager Secure Password Extension Administration Guide*.

- Users who self-register for the Web Portal, receive a confirmation email with a link to a confirmation page. On this page, the users can finish registering and set their initial password for logging in to One Identity Manager tools.

New configuration parameters: **QER | Attestation | ApproveNewExternalUsers**, **QER | Attestation | NewExternalUserTimeoutInHours**, **QER | Attestation | NewExternalUserFinalTimeoutInHours**, **QER | Attestation | MailTemplateIdents | NewExternalUserVerification** und **QER | WebPortal | PasswordResetURL**

New application role: **Base roles | Self-registered employees**

- Different status messages are now shown as browser messages.

New Web Designer configuration parameters: **VI_Common_EnableNotifications** and **VI_Common_NotificationPollingInterval**

Target system connection

- New Privileged Account Governance Module for managing Privileged Account Management systems in One Identity Manager.

You can create and edit user accounts in One Identity Manager. User accounts obtain user accounts that can request the entitlements required for accessing privileged systems in Privileged Account Management system. Request user accounts, user groups and access requirements to privileged systems in the Web Portal.

With the One Identity Safeguard connector, One Identity Safeguard appliance user accounts, user groups, assets, asset groups, asset accounts, directories, directory accounts, account groups, entitlements and access request policies can be loaded into One Identity Manager. This allows you to use Identity and Access Governance processes such as attesting, Identity Audit, user account and system entitlements management, IT Shop or report subscriptions for Privileged Account Management tenants.

For more detailed information, see the *One Identity Manager Administration Guide for Privileged Account Governance*.

- The Windows system monitor shows you performance data for target system synchronization. You can enable performance monitoring in the Synchronization Editor configuration file (`SynchronizationEditor.exe.config`). You must start the Synchronization Editor in administrator mode in order to select One Identity Manager performance indicators.
- Changes to a single object in the target system can immediately be transferred to the One Identity Manager database without having to synchronize the entire target system. Single object synchronization can be executed in Manager for objects that are already in the One Identity Manager database. The changes are made to the object properties that are mapped. If a membership list belongs to the object properties, the assignment table entries are also updated. If the object in the target system no longer exists, it is deleted in the One Identity Manager database.
- You can define cross-synchronization project start sequences for full synchronization. This allows you to order start up configurations for different target system in a sequence and they are synchronized one after the other. The configuration parameter **DPR | StartSequence | LifeTime** controls the retention period for completed start sequences.
- The native data connection allows you to extend the connector schema with virtual schema properties. A data operation that uses the virtual schema property must be defined for the relevant table. This schema property can then be precisely defined.
- The Synchronization Editor provides a script library. All the scripts defined here can be used in other synchronization project scripts. Scripts that are marked as script templates can be imported into other synchronization projects where you can modify them and continue to use them. The scripts of script properties can be moved into the script library.

- Before a G Suite user account is deleted, the user data can be transferred to another user account. The user account is not deleted from the target system until the data has been successfully transferred. You can configure this behavior in the target system connection. This function can only be used in newly created synchronization projects.
- Access permissions for central user administration's SAP child system can be guaranteed through direct assignment, IT Shop requests and indirect assignments. Account definitions are used to do this.

NOTE: Up to version 8.0, access to the central system was granted automatically (entry in table SAPUserInSAPMandant). As from version 8.1, this access must be explicitly granted (entry in SAPUserMandant). Existing assignments in SAPUserMandant are converted into direct assignments during the One Identity Manager database migration. This way, access permissions to the central system remain intact.

Patches with the patch IDs VPR#28147 and VPR#28147_2 are available for synchronization projects.

- SAP parameters can be passed down to SAP user accounts through business roles and organizations.

Identity and Access Governance

- Managers of system roles, applications and subscribable reports can edit requests for objects of this type in the Web Portal. For this to work, managers are automatically added to the new application roles for product owners of system roles, applications and subscribable reports.
- New configuration parameter under **QER | Person | Starling** for supporting One Identity Hybrid Subscription.

See also:

- [Enhancements](#) on page 8
- [Resolved issues](#) on page 27
- [Schema changes](#) on page 45
- [Patches for synchronization projects](#) on page 54

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.1.

Table 1: General known issues

| Enhancement | Issue ID |
|---|-------------------------------------|
| In the case of process tasks and processes, you can define whether to wait for DBQueue Processor tasks to be handled. | 28087 |
| Improved report generation. <ul style="list-style-type: none"> You can now use the Escape button to stop a report from being generated. The process component ReportComponent has a new parameter LimitRows, which defines a maximum limit for the number of lines returned for each query. | 28921, 17407, 15696 |
| Improved report export. <ul style="list-style-type: none"> There is a new parameter for the process task Export, process component ReportComponent, which exports reports as Microsoft excel files. There is now a parameter for the process task SendRichMail, process component MailComponent, which allows you to send reports in different formats as mail attachments. | 19107 |
| Improved reports with historical data queries. <ul style="list-style-type: none"> The Historical assignments query module allows queries to be created that are based on foreign key objects. In the Historical assignments and Multiple object history query modules, you can specify which columns have their modifications displayed in the report. You can define several criteria for the query modules Historical assignments and Multiple object history. The data query for the query module Historical assignments returns the columns Origin and OriginDisplay for querying assignment types. | 21158, 21159, 22003, 29816 |
| Improved assignment of method definitions (DialogMethod) to object definitions (DialogObject). | 30462, 30514 |
| Detailed license report in the License Meter. | 30321 |
| Improved support for data transport. <ul style="list-style-type: none"> When using the Database Transporter export function, you can select change labels under a root change label. New dialog for solving transport conflicts. New transport mode for transporting synchronization projects. | 12732, 28945, 29555 |
| In the Process Editor, the \$ notation suggestion list has been extended. The | 16108, |

| Enhancement | Issue ID |
|--|---|
| \$PC(VarName>)\$ input shows an example in the suggestion list. The values(input shows a suggestion list with value definitions. The "&out(input shows a suggestion list with out parameters. | 29090 |
| To access the display value of column's old value, you can combine the object properties [o] and [d]. | 19641, 17262 |
| Custom configuration parameters can only be created under the configuration parameter Custom . | 30764 |
| <p>i NOTE: Existing custom configuration parameters cannot be customized on grounds of compatibility. Adjust these configuration parameters manually if required and check their usage.</p> | |
| Improved indexing of the search index. <ul style="list-style-type: none"> You can use the configuration parameters Common Indexing BatchSize and Common Indexing Interval to configure the search index. If the application pool is being reused, the search index is read-only. Indexing log messages about are written to the application server's log. | 786112, 30436, 30065 |
| Improved logging in the program Quantum.MigratorCmd.exe. | 30412 |
| You can use the configuration parameter QBM DBServerAgent CreateNotification to specify when messages are written from SQL Server Agent tasks to the event log. | 30376 |
| The process component HandleObjectComponent's process tasks have been extended by an optional parameter ProcID for passing the GenProcID. | 30323 |
| <p>i NOTE: The default processes have been modified. You must manually modify your custom processes as necessary.</p> | |
| The last process collection time for a Job server is saved. | 30270 |
| Improved feedback from consistency checks. | 30193 |
| You only see a selection of system types for a new connection in the database connection's login if different system types are allowed. | 30124 |
| Improved navigation and editing of objects in Designer. Improved displaying of custom changes in Designer. | 29864, 29786, 28997, 29001, 29342, 23814 |

| Enhancement | Issue ID |
|---|---------------------------|
| Improved update behavior for automatic software update. | 29886 |
| You can disable authentication module assignments to applications. | 29878 |
| You can also set the time in the control for setting the date. | 29870 |
| Forms with the form template FrmCommonChildRelationGrid show a column tooltip in the table header. | 29022 |
| There is a spell checker in the Designer's Language Editor. | 29252 |
| In the change label dialog, you can filter by change label. | 24098 |
| Specialized editor for certain configuration parameters. | 29751 |
| The VI.Base.ViException class now has a function SetSolution for setting the parameter and the text key plus a parameter, Solution, to load the completed text for entering in a solution to a problem. | 29433 |
| The process tasks SendMail and SendRichMail of the process component MainComponent have been extended by the parameter TransportSecurity for specifying the encryption method for sending notifications by mail. The parameters EnableSSL, StartTls, StartTlsWhenAvailable and NoTransportSecurity have been deleted. | 29662 |
| <p>i NOTE: The default processes have been modified. You must manually modify your custom processes as necessary.</p> | |
| <p>Improved support for deferred operations.</p> <ul style="list-style-type: none"> • The menu item Database Show deferred operations is always shown in the Manager now. • On assignment forms, deferred operations for assignments are marked with their own icon. • Additional configuration parameters for configuring deferred operations are Common DeferredOperation AllowUpdateInInsertMode and Common DeferredOperation IgnoreMissingOnDelete. | 21663, 30215, 30734 |
| Improved execution of templates through One Identity Manager Service. | 22360, 30730 |
| <p>Support for dynamically created HTML code in mail templates. It can be marked as type HTML in \$ notation. The HTML code is accepted in scripts and columns but not masked. There is no security check.</p> <p>Example script with HTML code:</p> <pre>Public Function CCC_HtmlMailText(obj As IEntity) As String Return "<h1 style='color:red'>" & obj.Display & "</h1>"</pre> | 27806 |

| Enhancement | Issue ID |
|---|--|
| <p>End Function</p> <p>Call in mail template:</p> <pre>\$SCRIPT(CCC_HtmlMailText):HTML\$</pre> | |
| <p>Improvements in Job Queue Info.</p> <ul style="list-style-type: none"> The Affected objects view shows all the objects affected by a process step. The Progress view shows the reinitialized Job queue. There is a warning in Job Queue Info as well. By clicking on the message, more detailed information is shown. You can multi-select parameters for copying. If the DBQueue contains more than 250000 calculation tasks, the operation There are more tasks to be processed is displayed in the DBQueue. This shows the number of queued tasks that cannot currently be shown in the DBQueue overview. | <p>29052, 16641, 28692, 31140</p> |
| <p>Improvements in the Configuration Wizard.</p> <ul style="list-style-type: none"> Improved checking of SQL Server and database settings in the Configuration Wizard before migrating a One Identity Manager database. The module version is displayed when you select the module. If you create a new database with the Configuration Wizard, the directory name is also displayed if you select <default>. Improved error list in the Configuration Wizard. | <p>29224, 29262, 30227, 22575, 31061</p> |
| <p>Additional consistency check Differences in usage types in referring tables to prevent transport problems.</p> | <p>29803</p> |
| <p>Improved selection of values from a list of permitted values in the Where Clause Wizard.</p> | <p>29024</p> |
| <p>The simulation of permissions in Designer can be limited to selected tables.</p> | <p>29273</p> |
| <p>Tables of type Read only, Union and Proxy can only be defined as viewable.</p> | <p>29500</p> |
| <p>Improved support for statistics.</p> <ul style="list-style-type: none"> New editor for editing statistic definitions in Designer. The statistics control has been extended. By double clicking on the title bar of a statistic, you can open other menu items to display reports or lists, for example. Another menu item must be defined below the menu item to get this functionality. | <p>29444, 29145</p> |
| <p>Initialization of auto-completion for entering script code is now done in the background.</p> | <p>29713</p> |

| Enhancement | Issue ID |
|--|---|
| Process ID and start times of external processes are displayed on the One Identity Manager Service website. | 29718 |
| Improved support for loading web application files in Software Loader. | 29770 |
| New process tasks for setting and removing access rights for the process component FileComponent. | 29791 |
| The number of list elements for data dependent menu items in a list are now shown. | 30383 |
| You can configure how long the value of process parameters are allowed to be, which are recorded in the process history. New configuration parameter: Common ProcessState JobHistory TrimLongParameters | 29606 |
| On table relations, you can specify whether the root object, in a list of affected objects from a process, is added. This can prevent the parent object from being processed simultaneously more than once. | 29421 |
| Optimization of object selection scripts for objects in the table BaseTree. | 22266 |
| The overview forms VI_Structure_Locality_Assignments_Overview, VI_Structure_Department_Assignments_Overview, VI_Structure_ProfitCenter_Assignments_Overview and VI_Structure_Org_Assignments_Overview have been deleted. | 28988 |
| The Designer's Schedule Editor can now be started from Launchpad. | 29045 |
| The schedules Lock accounts of employees that have left the company and Enable temporarily disabled accounts are not enabled by default. | 29045 |
| Employees and system users that are locked due to incorrect logins, are displayed in Manager and Designer. <ul style="list-style-type: none"> • New menu items in the navigation structure • Tooltip on overview forms | 29095, 29371 |
| The Person.OrderShoppingCart method interface has been changed to improve support for application servers. The class QER.Customizer.ItemInfo now contains ExceptionInfo with detailed information about the error. | 29928 |
| Improvements in the application server <ul style="list-style-type: none"> • Improved protection of the application server's API. • Improved logging in the application server. • Improved validation of application server connections. | 30405, 30618, 30315, 31299, 31300 |
| Improved performance in DBQueue Processor. | 30763, 30800, 30626 |

| Enhancement | Issue ID |
|--|---------------------------|
| Improvements in the system information overview. <ul style="list-style-type: none"> Improved display of recommendations for settings and critical values are highlighted. Some of the database server's properties for the system information overview are determined by the DBQueue Processor depending on the configuration parameter QBM DBServerProperties. | 30896, 30678, 30850 |
| Improved logging in the process component MailComponent. | 31043 |
| Release management support. There is a new change label type Release for collecting change labels for a release and additional reports in Designer. | 29119 |
| One Identity Redistributable STS updated to version 2019.1.1.11. | 30981 |
| The Report Editor uses Stimulsoft Ultimate 2019.1.1. | 769216, 30873 |
| Performance optimization when string instances are reused. | 30341 |
| The connection server already provided for transferring data to a One Identity Manager History Database is now used. To use this function, enable the configuration parameter HDB UseNamedLinkedServer in the One Identity Manager History Database and enter the connection server in the One Identity Manager History Database as server for the source database. | 30028 |
| Error messages from the process history are transferred to the One Identity Manager History Database. | 29147 |
| Improved logging of error messages when transferring data to the One Identity Manager History Database. | 30165 |
| Improved performance when updating the One Identity Manager database. | 30292 |
| The script VID_FindAndReplaceByLine has been deleted. | 30632 |
| Implementation of a load cache ISession.QueryCacheBlock() to load SQL queries that might be called more than once, in one block. | 27856, 29705 |
| Improved protection against damaging SQL statements. | 31299, 31301 |

Table 2: General web applications

| Enhancement | Issue ID |
|--|---|
| Improved performance in the Web Portal for: <ul style="list-style-type: none"> Displaying delegations, requests for approval and the request history Editing questions about attestation cases | 770382, 29414, 30470, 30471, 30673, |

| Enhancement | Issue ID |
|---|---|
| <ul style="list-style-type: none"> Determining an employee's entitlements Approving requests | 30863, 31192 |
| You can select the language on the login page before logging in. | 781956 |
| Web Portal users can specify their language preferences when they register. | 795283 |
| If the first login to the Web Portal fails because the confirmation link has expired, for example, the user can request a new confirmation email. | 30812 |
| <p>Improved user navigation in the Web Portal.</p> <ul style="list-style-type: none"> The page Responsibilities Auditing has been structurally reworked. The way some parameters are displayed in the filter wizard has been made more user friendly. List sort order (DialogTree.ListOrderBy) is taken in to account in Hyper Views in the Web Portal. The detail view and overview tiles for business and system roles show more information. Improved display of potential rule violations. Improved display of URL in property view. The page My Processes has been reworked and improved. The search is shown in another view. Hyper Views display additional information. | 726106, 738158, 745500, 760498, 761671, 762208, 768037, 773368, 773566, 775573, 781813, 783457, 30034 |
| <p>Improved user navigation for editing and approving requests.</p> <ul style="list-style-type: none"> The 'Save for later list' can be completely deleted with one click. After moving the last product from the 'Save for later list', the user is automatically shown the shopping cart. After moving the last product from the shopping cart to the 'Save for later list', the user is automatically shown the 'Save for later list'. It is now easier to navigate to objects in the request history detail that are linked to the request. Improved display of service categories when you make a request. If a user clicks on the email link to make an approval decision about a request and the decision has already been made, the user is notified by a message in the Web Portal. The Requests for <user> page offers a selection of recipients if | 738155, 738157, 740766, 746966, 769201, 769896, 775198, 784674, 786514, 794762, 795801 |

| Enhancement | Issue ID |
|--|-----------------------------|
| <p>there is more than one for the request.</p> <ul style="list-style-type: none"> The view of request to be approved is now sorted by priority. In the request history, you can translate information about request time and date. In the request overview, the request can subsequently be sorted and filtered. The selection specifying which requests are copied, resent or added to a request template, has been reworked. | |
| When requesting products, you are shown whether a product has already been requested. Products that have already been requested cannot be added to the shopping cart again. | 736902, 25756 |
| If a custom request property is identical to a default request property (such as the valid from date), only the custom request property is shown in the shopping cart. | 29305, 743621 |
| The test to find out what products an employee is allowed to request has been extended in the AccProductInDepartment table. | 748251 |
| With the new Web Designer configuration parameter VI_ITShop_Employee_Preselected , you can specify whether the current user is always preselected as recipient for a new request. | 748875 |
| The default value for extending a request is now a value in the future and can be configured with help from the Web Designer configuration parameters VI_ITShop_Prolongation_Offset . | 738195, 26139 |
| <p>Improved user navigation when attesting with automatic removal of entitlements.</p> <ul style="list-style-type: none"> The mail templates contain a link to the details of the attestation case and a warning if entitlements are removed automatically when the attestation case is not approved. The attestor sees various details of the entitlements that are removed automatically. | 736904, 794742, 30893 |
| Web Portal users can view details of all the attestation cases that affect them. | 30325 |
| New tab Compliance on the Pending attestations page. Detailed information is shown about rule violations of attestation objects. | 783486 |
| If the option Employees do not inherit is set on a role, the user is informed of potential rule violations while compliance checking this role or during direct assignment. The rules will be violated the moment the option Employees do not inherit is disabled. | 760181, 25477 |

| Enhancement | Issue ID |
|---|---|
| When resolving rule violation, SAP roles that match SAP functions are taken into account. | 782806 |
| If, during resolution of rule violations, no permissions are found on the first page, a better error text is displayed. | 787292 |
| Users with the application role Identity Management Employees Administrators can now also manage employees in the Web Portal. | 715356 |
| Selecting employees or user accounts also shows the identity. | 28878 |
| The filter wizard is only shown for users with the program function Allow use of SQL wizard in Web Portal (Common_SqlWizardWeb). | 792338, 30240 |
| In tables that display hierarchical objects, the number of entries is shown at the top level. | 758936 |
| In the Web Portal, some parts of Hyper Views are hidden. | 764013 |
| The session in Web Portal can now be closed through a fixed URL <code>/page.axd?ContextID=QBM_Logout</code> . | 771671 |
| Until now, missing form methods were entered as errors in the log. This error will now be ignored because during normal operations there are too many incorrect error messages due to the overlapping timing of user actions. | 30373 |
| Certain error messages offer suggestions for solving the problem. | 785123 |
| The Web Designer configuration parameter VI_Common_AutoCompleteListCount allows the user to specify how many matches are displayed for auto completion. | 670646 |
| The new Web Designer configuration parameter VI_Common_HyperView_DisableNavigation allows you to disable navigation to other objects. | 779809 |
| The new Web Designer configuration parameter VI_Common_AutoCompletePrefixOnly allows you to specify whether only matches that begin or contain the given term are displayed by auto-complete in input fields. | 780465 |
| The new Web Designer configuration parameter VI_Common_CaptchaCaseInsensitive allows you to specify whether case sensitivity is checked by Captcha. | 785849 |
| Employees, who are noted in the system as inactive with certification status new , can also log in to the Password Reset Portal. | 30742 |
| Improved user navigation in the Password Reset Portal. <ul style="list-style-type: none"> You can return to the home page at any time. On the login page, you can configure the language before logging | 724499, 759436, 789656, 794857 |

| Enhancement | Issue ID |
|--|--|
| <p>in.</p> <ul style="list-style-type: none"> • Password questions and answers can also be set and changed in the Password Reset Portal. • Users can also change their sub identity passwords in Password Reset Portal. | |
| In the Operations Support Web Portal, you can limit the search to objects in specific tables. | 772962 |
| <p>Improved user navigation in Web Designer.</p> <ul style="list-style-type: none"> • The design has been reworked. • The help menu has been reworked. • Terminology for saving projects has been changed. Project type is now used instead of save type. • The search function has been renamed to Find in the English user interface. • The information about the current object is now displayed in the toolbar instead of the node editor. | 771460, 781812, 785007, 786212, 787063 |
| A new property has been added to nodes at hierarchical level. It controls which nodes expand automatically when the data is loaded. | 789080 |
| It is now possible to jump straight from a report to the overview pages of separate entries. | 691041 |
| The EditFilter() function in the Web Designer component VI_Edit_LimitedValues has been removed. You can only make changes to limit permitted values by using the properties. | 787115 |
| The Web Designer component VI_Audit_Responsibilities uses the database view TSBVUNSRoot for displaying. | 763281 |
| Microsoft Edge can now be started from Web Designer. | 750375 |
| Object dependent references can be edited and disabled in Web Designer. | 753696, 753699, 29313 |
| The script for displaying the status of menu items (DialogTree.StateScript) is also taken into account by Web Designer. | 29989 |
| Comments can now be added directly or by extension to collections. | 709434 |
| The Web Designer Configuration Editor now checks whether a user account exists for automatic update and that the login data is correct. If this is not the case, the user can create a new user account. | 736495 |
| Changes to files that are not made in Web Designer, are no longer | 762527 |

| Enhancement | Issue ID |
|---|-------------------|
| overwritten by saving in the Web Designer. | |
| Web Designer compiler messages can be identified more easily based on error codes. In addition, the user can specify which warnings are handled as error and which error codes should be ignored. | 780370, 780371 |
| The log file display has been reworked in the Web Portal. | 741876 |
| In the web application's log file, the list Web Designer nodes are shown with IDs. | 766259 |
| Direct HTTP calls to Starling 2FA API are no longer possible. The QER.DefenderClient.dll has been renamed to QER.Starling2FAClient.dll. | 720212 |
| The Starling 2FA client API version 5.9.18078.3 is supported. Modified scripts: QER_CreateMFAUserID and QER_DeleteMFAUserID | 767068, 770670 |
| To prevent a Cross-Site-Request-Forgery (CSRF), the attribute SameSite for cookies with the value strict is preset in the Web Portal installation. | 777728 |
| To guarantee more security, the default file web.config has been extended by the parameter httpRuntime enableVersionHeader="false". | 736623 |
| AngularJS 1.7.2 is used. | 774246 |
| If a user uses a user interface with high contrast, selected table entries are highlighted with a frame. | 738193 |

Table 3: Target system connection

| Enhancement | Issue ID |
|---|-----------------|
| Obsolete synchronization revisions are deleted by daily maintenance tasks in the table DPRRevisionStore. | 22602 |
| Maintenance of the synchronization buffer can be done manually in the Synchronization Editor's expert mode. | 24438 |
| Optimization of data throughput during provisioning if an application server is used. | 27347 |
| While setting up a synchronization project from a custom project template, the synchronization project wizard adds single object operations for provisioning and for single object synchronization. | 28280 |
| Improved representation of outstanding membership objects on the overview form for target system objects. | 28491, 19817 |
| Single provisioning can also be implemented with value comparison rules that map multi-value schema properties. | 28759 |
| In the schema properties for resolving keys, you can configure whether | 29092 |

| Enhancement | Issue ID |
|--|---|
| unresolvable keys are written to the synchronization log. | |
| Schema properties for resolving keys can be defined as Read-only . | 29171 |
| A manager assignment to an employee can be removed by synchronizing Oracle E-Business Suite. A manager assignment to a department can be removed by synchronizing an SAP HCM system. | 29265 |
| A patch with the patch ID VPR#29265 is available for synchronization projects. | |
| Improved user navigation in the Synchronization Editor. <ul style="list-style-type: none"> • Improved display of member lists in the target system browser. You can sort the objects displayed in the schema properties edit dialog. • Detailed information is displayed about the results of the consistency check. • In the Synchronization Editor, when a user opens a synchronization project a message appears if another user is already working with this synchronization project. • By activating and saving already active synchronization projects, the consistency check is automatically run. If errors occur, the user will be prompted to activate or save the synchronization project. • Improved display of the scope in the Synchronization Editor. • Improvements in the Select system connection dialog when the synchronization project is created. • In the target system browser, the filter for displaying the result list for the selected schema type can be defined before the list is loaded. | 24317, 29258, 29334, 29363, 29396, 29957, 30197 |
| New consistency checks have been implemented. <ul style="list-style-type: none"> • Property mapping rule checking • Check whether start up configurations that have been grouped into a start group use the same schedule. • Check whether schema properties are in use that are marked internally as obsolete. | 29642, 30654, 30780 |
| Improved error message when a synchronization project cannot be opened because the scripts being used contain syntax errors. | 29947 |
| In the target system browser, system objects can be displayed that contain encrypted values. | 30021 |
| Synchronization projects can be automatically updated. The configuration file can be provided through a reference object. | 30416 |

| Enhancement | Issue ID |
|---|---|
| Script properties can be configured so that script runtime errors are ignored. | 30591 |
| Improved performance <ul style="list-style-type: none"> • Single provisioning of memberships • Calculating DBQueue Processor tasks • Synchronizing • Provisioning new objects with Windows PowerShell based connectors | 22556, 29063, 30667, 30702, 30864, 30892, 30922, 30942 |
| Synchronization logs are shown in Manager. | 30949 |
| Additional object definition for displaying user accounts in Manager depending on the respective identity. | 27038 |
| The forest relation is mapped to Active Directory locations. A patch with the patch ID VPR#29306 is available for synchronization projects. | 29306 |
| The options Password never expires and Change password on next login for Active Directory user accounts cannot be enabled at the same time anymore. | 30521 |
| When Active Directory user accounts are synchronized, references to cloud user accounts are synchronized. Synchronization is supported by the Active Directory and Active Roles connectors. A patch with the patch ID VPR#29087 is available for synchronization projects. | 29087 |
| During synchronization with the Active Roles connector, information about the Active Directory operating system is loaded. A patch with the patch ID VPR#28612 is available for synchronization projects. | 28612 |
| The Azure Active Directory connector uses Microsoft Graph .NET Wrapper Version 1.6.2. | 28801 |
| The configuration parameter Target system AzureAD is a preprocessor configuration parameter. | 30485 |
| Microsoft Exchange room mailboxes can be created for enabled Active Directory user accounts. | 28222 |
| The mailbox type of Microsoft Exchange mailboxes can be changed. | 30569 |
| Proxy addresses can be maintained for remote mailboxes. | 29949 |
| Remote mailboxes with the mailbox type Remote shared mailbox can be created. | 30252 |

| Enhancement | Issue ID |
|--|-----------------|
| When a mailbox is enabled, there is a test to check whether a remote mailbox or an e-mail user already exists for the given Active Directory account. | 31126 |
| Property mapping rules that are no longer required are removed from the OwaMailboxPolicy map. A patch with the patch ID VPR# 30498 is available for synchronization projects. | 30498 |
| Booking permissions for Exchange Online room and equipment mailboxes can now be granted for dynamic distribution groups, mail-enabled distribution groups and Office 365 groups. A patch with the patch ID VPR# 30588 is available for synchronization projects. | 30588 |
| The following messages have been added to the list of errors caused by a dropped connection: An error caused a change in the current set of domain controllers. Your request is too frequent. Please wait for few minutes and retry. Topology Provider couldn't find the Microsoft Exchange Active Directory Topology service on end point. | 31168 |
| Improved performance synchronizing Exchange Online recipient lists. | 30959, 31162 |
| Primary memberships of employees in locations are also synchronized. A patch with the patch ID VPR# 29741 is available for synchronization projects. | 29741 |
| In the system connection wizard, schema extension files for Oracle E-Business Suite are also checked for functional errors. | 30402 |
| The Oracle Database Edition can be selected when setting up synchronization for E-Business Suite. The Edition can be changed in the connection parameters at any time. A patch with the patch ID VPR# 30464 is available for synchronization projects. | 30464 |
| The serialization format of schema types in synchronization projects can be changed for Oracle E-Business Suite. A patch with the patch ID VPR# 31011 is available for synchronization projects. | 31011 |
| Read-only API access can be configured for synchronizing G Suite. | 29934 |
| In Manager, the G Suite organization property Block inheritance (GAPOrgUnit.BlockInheritance) cannot be edited anymore because it cannot | 30452 |

| Enhancement | Issue ID |
|---|-------------------------------------|
| edited with the Google Admin Console either. Do not use this property anymore. | |
| The G Suite connector uses Google.Apis version 1.37.0. | 30979 |
| Option to redefine structural classes as auxiliary classes in the LDAP connector. | 20824 |
| Spaces in distinguished names of LDAP objects are tolerated. | 30542, 30543 |
| Automatic partitioned search for LDAP server with Oracle Directory Server Enterprise Edition (ODSEE) is no longer supported. The partitioned search can be configured in the system connection wizard. To do this, select the object class nsUniqueId on the Options for partitioned search page and use the characters ABCDEF0123456789 . | 30733 |
| When adding Notes mailbox files, you can set an access step for the owner. The configuration parameter TargetSystem NDO Accounts MailFileAccessRole specifies which access steps are passed by default. A patch with the patch ID VPR#30313 is available for synchronization projects. | 30313 |
| Improved performance <ul style="list-style-type: none"> • Provisioning Notes objects • Provisioning Notes group memberships | 30658, 30895 |
| Parameter of type IN can now be passed to the process task RunAgent of the process component NDO Component . | 30856 |
| The communications timeout between SharePoint connector and target system has been increased to 24 hours. | 30804 |
| The configuration parameter Target system SharePoint Online is a preprocessor configuration parameter. | 30486 |
| SAP user accounts can be renamed in One Identity Manager. In the process, the user account properties are transferred to a new user account and the original user account is deleted. | 29285 |
| In the system connection wizard, schema extension files for SAP R/3 are also checked for functional errors. | 30304 |
| Improved performance <ul style="list-style-type: none"> • Calculating SAP functions • Calculating SAP group, role and profile hierarchies. • Synchronizing role assignments with the central system of a CUA (UserInCUARole) | 30299, 30743, 30675, 30941 |

| Enhancement | Issue ID |
|--|-----------------|
| A patch with the patch ID VPR#30941 is available for synchronization projects. | |
| The process component SAP Component has been extended by the process functions ObjectExists and DelRoleFromUser. | 31120, 31145 |
| The SCIM connector can use client certificates for authentication. | 30154 |
| Variables used by synchronization and their values are logged. | 30190 |
| In synchronization projects with the SCIM connector, you can configure the use of local cache. | 30497 |
| A patch with the patch ID VPR#30497 is available for synchronization projects. | |
| The CSV connector recognizes multiple identical entries in the CSV file. For synchronization, you can select one entry or ignore all entries. | 30716 |
| Extended consistency checks in the Windows PowerShell connector. | 29201, 30220 |
| If a dropped connection is identified in a Windows PowerShell connector, the error message for the exception that caused it is outputted by NLog on each reconnection attempt. | 31164 |

Table 4: Identity and Access Governance

| Enhancement | Issue ID |
|---|---------------------------|
| <p>Simplified support of special processes for deleting employees during implementation of data protection regulations (GDPR).</p> <ul style="list-style-type: none"> A new procedure QER_PPersonDelete_GDPR is available. The process task Delete of the process component HandleObjectComponent has a new parameter Deep for deleting dependent objects and references. | 27643, 30468, 30721 |
| The delegator can be notified by the approval decision. | 20893 |
| If memberships in roles and organizations are attested (table PersonInBaseTree), the approval procedure CM can be used to determine the attestors. | 30123 |
| If the attestation procedure in an attestation policy changes, a check is done to find out whether the assigned approval policy is permitted. | 30218 |
| You can configure which methods are applied to a request if the requested assignment has to be removed because the attestation case was not approved. New configuration parameter: QER Attestation AutoRemovalScope PWOMethodName | 30581 |

| Enhancement | Issue ID |
|--|------------------|
| The approval procedure OA can also be used to determine an attestor if system entitlement assignments to user accounts or system role assignments to employees are attested. | 30636 |
| New approval procedure for determining attestors for user accounts: EA - user account's employee. | 30871 |
| Usage types can be assigned to standard reasons. In Web Portal, standard reasons are filtered this way. All usage types are assigned to your custom standard reasons during the One Identity Manager update. You can edit these usage types in Manager. | 22810, 789946 |
| In the approval step, you specify whether employees that are affected by the approval are allowed to approve this approval step. This prevents <ul style="list-style-type: none"> • The requester and recipient of one request making the approval decision • The employee being attested from approving the attestation case | 24141 |
| Default approval procedures can be copied for customization. | 24176 |
| Mail templates for renewal and unsubscribing can now be assigned to approval policies. The configuration parameter QER ITShop MailTemplateIds InformRecipientAboutUnsubscribe has been deleted. | 27142 |
| New mail templates for delegation approval notifications. New configuration parameters have been added under QER ITShop Delegation MailTemplateIds for configuring such notifications. | 27349 |
| When the recipient of a request is removed from a customer node, requested company resource assignments to business role and organizations can remain intact. New configuration parameters have been added under QER ITShop ReplaceAssignmentRequestOnLeaveCU for configuring this behavior. | 27640 |
| Improved performance calculating delegations. | 28964 |
| The method <code>CreateITShopOrder</code> already creates an entry in the approval sequence when the request is made in IT Shop. | 30368 |
| The task Remove from all shelves is only displayed if an IT Shop shelf is assigned to a company resource as a product. | 30382 |
| The configuration parameter QER ITShop LimitOfNodeCheck specifies how many product nodes are deleted in one DBQueue Processor run if large numbers of products in the IT Shop are deleted through automatic processes. By default, 500 objects are processed in one run. Set the value lower if there are performance problems while executing the task <code>QER-K-OrgAutoChild</code> . | 30657 |
| Unused application roles for product owners are now deleted if the configuration parameter QER ITShop GroupAutoPublish is not set. | 30796 |

| Enhancement | Issue ID |
|--|---------------|
| Improved performance handling request processes. | 30990 |
| Improvements calculating inheritance for system roles. <ul style="list-style-type: none"> New configuration parameter for defining mutually exclusive system roles: QER Structures Inherit ESetExclusion. Special handling of system roles are passed down through hierarchical roles. New configuration parameter: QER Structures Inherit NoESetSplitting | 28248, 28973 |
| On the system role overview, company resources that are assigned to child system roles are displayed in separate form elements. | 30737 |
| If affected permissions are specified in the rule conditions of compliance rules, you can define the partial conditions Has extended property in group and SQL statement . | 29100 |
| Improved display of rule violations involving SAP functions. <ul style="list-style-type: none"> New overview form with details about an employee's rule violations, the object involved and the mitigating controls assigned. The SAP functions affected and the compliance rules that can be violated by them are displayed on the overview forms SAP user accounts, SAP roles and SAP profiles, business role and organizations. The SAP function instance overview form shows the violated compliance rules and those business roles and organizations affected. | 29376 |
| An employee type can be given for employees. This represents the employee's relationship to the company. | 787290, 29094 |
| Reports about employees contain additional information. | 30063, 30079 |
| If the option Temporarily disabled is not set for an employee and the date for Temporarily disabled from is in the future, the date for Temporarily disabled from and Temporarily disabled until are not deleted. | 30344 |
| If a permanently disabled employee is re-enabled, the leaving date and last working day are only deleted if they are in the past. | 30993 |
| Role types can be assigned to role classes. This allows you to limit usage of role types to the assigned role classes. | 28131 |
| You can assign a manager and a deputy manager to an application role. | 29228 |
| Improved performance finding owners of system entitlements. | 30223 |

See also:

- [Schema changes](#) on page 45
- [Patches for synchronization projects](#) on page 54

Resolved issues

The following is a list of solved problems in this version.

Table 5: General known issues

| Resolved issue | Issue ID |
|--|----------|
| Populating raw tables fails if process views with identical process group IDs exist in the One Identity Manager database and the History Database as well. | 27846 |
| Error filling raw tables if the One Identity Manager database and the History Database are installed in the same cluster. | 30455 |
| The One Identity Manager History Service and the One Identity Manager Service are both installed when the One Identity Manager History Database is installed. To correct the problem, the HDBService.exe file has been removed. The installation of the History Database service will now be carried out by the viNetworkService.exe. | 28058 |
| i IMPORTANT: If you are affected by this problem, uninstall the One Identity Manager History Service before updating your One Identity Manager History Database. Run the following command as administrator: <pre>sc delete "HDBService"</pre> | |
| Error testing email addresses for uniqueness, if an email address was recalculated with a template but the old and the new values are identical. | 30300 |
| You can set edit permissions for columns that are part of a primary key or part of a key for a many-to-all table. | 29031 |
| Error message calling Quantum.MigratorCmd.exe with the operation DUMP. | 30305 |
| Problem opening Language Editor in Designer if very large tables are loaded for translation. | 30319 |
| The function QBM_FSQRemoveComment does not recognize Linux carriage return. | 30342 |
| The script for selecting the server in a process step (Job.ServerDetectScript) is not implicitly extended by a Try-Catch-Block. | 30347 |
| Bulk operations are obstructed from delivering process steps by entries in the QBMElementAffectedByJob table. | 30362 |

| Resolved issue | Issue ID |
|--|-----------------|
| If an object column and another column in the table <code>QBMCColumnTranslation</code> are interrelated, the program exits because it cannot load these objects. | 30380 |
| Compilation fails if the process or process step contains quotation marks (") in names. | 30403 |
| Error logging in through an application server if the user is working with Turkish language settings. | 30445 |
| Session ID in the application server can be reused. | 31299, 31306 |
| <p>i NOTE: Now the session ID is not reused, by default.</p> <p>You can configure reuse of the session ID. In the application server's configuration file (<code>web.config</code>), a new parameter <code>allowsessionidreuse</code> has been added to the section <code>server</code>. The modification only affects new installations. Existing installations are not changed.</p> <p>To allow reuse of session IDs:</p> <ul style="list-style-type: none"> • For new installations: uncomment the parameter in the application server's <code>web.config</code>. • For the existing installation: add the following to the <code>server</code> section of the application server's <code>web.config</code> <pre><add key="allowsessionidreuse" value="true" /></pre> | |
| Under certain conditions, the database ends up in a trigger-free state if transport fails. | 30459, 30447 |
| Performance problems determining permissions. | 30471 |
| Wrong name of state "Newfoundland and Labrador". | 30484 |
| After extending the schema of custom read-only tables, new columns with the option Customer can configure are set to the value 0 . | 30491 |
| Error in the method <code>SqlFormatter.NotInClause</code> . | 30505 |
| Problems initializing the Job queue if a large number of queues are affected. | 30539 |
| The physical dependency between <code>DBQueue Processor</code> tasks does not consider tasks without parameters. | 30573 |
| Terminated slots are identified correctly if the SQL Server reuses the SPID. | 30584 |
| The procedures for shrinking the entries in the tables <code>DialogWatchOperation</code> , <code>JobHistory</code> and <code>DialogProcessChain</code> do not shrink in blocks. | 30604 |
| Timestamps on changes made in the database in Designer are shown in UTC. | 30610 |
| Problem determining the resulting permissions filter for objects. | 30582, |

| Resolved issue | Issue ID |
|---|-----------------|
| | 31110 |
| Migration does not remove non-linear dependencies correctly. | 30693 |
| Error retrying process steps with the status MISSING . | 30752 |
| The procedure QBM_PCUSTOMSQLFill fails with the message Violation of PRIMARY KEY constraint. | 30753 |
| There is a new consistency check Index name longer than 30 characters . | |
| The customizer method getNextID fails when executed in Designer. | 30786 |
| Custom columns are not taken into account by auto-completion if script code is entered. | 30805 |
| If a process step is copied in the Process Editor, the priority definition (Job.PriorityDefinition) is not copied at the same time. | 30903 |
| If a Job destination ID contains a special character, the links on the One Identity Manager Service status page do not work. | 30924 |
| Ctrl+C does not copy the selected value in the Process step view in Job Queue Info. | 30343 |
| Job Queue Info ends unexpectedly, if there is a filter on the system journal and it returns a lot of entries. | 30928 |
| In reports, IN clause queries on UID and XObjectKey columns are listed with Unicode strings. | 30723 |
| The limit for IN clause in report queries is not kept to correctly. | 30724 |
| Relaying processes is being blocked because the procedure QBM_PJobUpdateState is being called to frequently. | 30798 |
| Error in process tracking (NullReferenceException). | 30978 |
| The state of Florida has the wrong timezone. | 31089 |
| The procedure ProcessShrink leaves behind entries with BasisObjectType=<unknown Object> in the DialogProcess table. | 31007 |
| Components and tasks with MaxInstance=1 run in parallel due to load balancing. | 29577 |
| Triggers are not generated for DBQueue Processor tasks that record changes to configuration data. | 30646 |
| The One Identity Manager Service returns the process steps but the slots remain blocked. | 31055 |

Table 6: General web applications

| Resolved issue | Issue ID |
|---|-----------------|
| Error logging in to the Password Reset Portal again if the portal was not in use in the meantime. | 30423 |
| Unsuitable error message if a password is entered in the Password Reset Portal that does not conform to the password policy. | 29804 |
| An employee can request membership in a specific business role. | 30194 |
| Next has to be double clicked in each step of a delegation in Web Portal. | 30216 |
| Unsubscribed assignment requests are shown in the request history, although the option Canceled or denied or dismissed is not set. | 30726 |
| A request for a default service item New Active Directory security group cannot be approved. | 30837 |
| Mandatory fields for attestation cases are not checked when queried. | 30862 |
| If the Report Subscription Module is not installed or the configuration parameter QER RPS DefaultReportTemplate is not set, a PDF export is still offered in the Web Portal. Attempts to export to PDF in Web Portal fail. | 28160 |
| The web browser control in Web Designer blocks certain URLs. | 28626 |
| If you swap pages when trying to select of roles during delegation, you lose the selection. | 29861 |
| Incorrect where clauses are generated while index searching in many-to-many tables. | 30679 |
| In the Web Portal, the character sets are not translated in the password policy tip. | 30960 |
| Wrong display names for DialogSchedule.LastRun and DialogSchedule.NextRun in the Schedule Editor. | 30687 |
| In the Web Portal, the Memberships tile is shown if you select an assignment resource under Responsibilities , although a member could not be assigned to an assignment resource. | 29440 |
| Diagram pages that extend over several pages are not displayed correctly. | 737307 |
| Error if the Manager web application is called by a Load Balancer. | 31064 |

Resolved issue

Issue ID

i **NOTE:** By default, use of SameOrigin is enabled because it concerns a security function. Use of the SameOrigin Policy can now be optionally disabled. In the Manager web application's configuration file (Web.config), in the section application, insert the following entry to do this.

```
<application>
...
<add key="DoNotApplySameOriginPolicy" value="True" />
...
</application>
```

In the Web Portal's configuration file (web.config), the URL /AE.axd is still declared.

31299,
31302

The handler AE.axd for session information has been removed from the Web Portal's configuration file (web.config). Therefore, the handler is not included when Web Portal is installed. Any existing Web Portal installations are not affected by this change.

i **NOTE:** If you still require the handler and want to include it again, enter the following lines in the Web Portal's configuration file (web.config):

In the section system.web\httpHandlers:

```
<add verb="GET" path="AE.axd"
type="VI.WebRuntime.Communication.ControllerRequestHandler,
VI.WebRuntime" />
```

In the section system.webServer\httpHandlers:

```
<add name="AE.axd_GET" path="AE.axd" verb="GET"
type="VI.WebRuntime.Communication.ControllerRequestHandler,
VI.WebRuntime" />
```

Table 7: Target system connection

| Resolved issue | Issue ID |
|---|----------|
| Errors publishing group memberships if there are memberships that are not mapped. | 29691 |
| Error executing the script DPR_GetAdHocData. | 29847 |
| Property mapping rules with the option Force mapping against direction of synchronization are not fully included if provisioning executes several synchronization steps of workflow. | 29922 |

| Resolved issue | Issue ID |
|--|-----------------|
| If changes are made to group properties, too many post-processing tasks are queued in the DBQueue. | 30076 |
| If patches are being applied and the database has encrypted connection data, the connection dialog for entering the data, opens in the background. | 30162 |
| In Manager, changes to the value of IT operating data cannot be saved. | 30295, 30746 |
| Error opening master data form of object from custom target system if custom columns are displayed. | 30336 |
| It is not possible to remove a target system from the database with the procedure QBM_PDeleteDeep. | 30374 |
| The settings in a hierarchy filter that has been converted into a variable, are removed from the Synchronization Editor if the target system connection cannot be established. | 30391 |
| Files in the synchronization user's temporary directory are not deleted. | 30396 |
| Error reading data from columns with data type varbinary if these are used as a primary key or part of one. | 30474 |
| Error loading synchronization projects. | 30503 |
| Error in provisioning when decoding XML strings. | 30525 |
| Simulation results do not contain enough information. | 30550 |
| Provisioning tasks for group memberships are grouped under the wrong GenprocID. | 30565 |
| A maximum of 1024 modified memberships per group can be provisioned. | 30597 |
| Too many columns are loaded for resolving a reference. | 30600 |
| Running a clean up of the DPRMembershipAction table deletes entries that are still required. | 30603 |
| Synchronization deletes One Identity Manager database objects that are not unique in the target system. | 30715 |
| Processing of target system specific tasks in the DBQueue is blocked if this target system is being synchronized at the same time. | 30773 |
| Provisioning of group memberships fails if a referenced object is not found. | 30787 |
| Script variables are recalculated each time they are accessed. | 30864 |
| Objects that are added and provisioned in the One Identity Manager database while synchronization is running are duplicated in the database. | 30957 |

| Resolved issue | Issue ID |
|--|-----------------|
| One Identity Manager uses the wrong mapping to provision memberships. | 31024 |
| Updating the schema or transporting a synchronization project removes the quota definition. | 31098 |
| The synchronization user's password is written to the log file without encryption. | 31112 |
| Synchronization start up loads the variable set too late. | 31152 |
| Post-processing tasks for outstanding objects that have been deferred, are not executed. | 31180 |
| Incorrect handling of trusted domains in Active Directory synchronization projects. The project template has been corrected. A patch with the patch ID VPR#30192 is available for synchronization projects. | 30192 |
| Cross domain memberships are not deleted during provisioning. | 30256 |
| Active Directory group memberships are not provisioned if the object SID for the user account is missing. | 30509 |
| Error processing unresolvable keys during Active Directory synchronization. | 30552, 30811 |
| Deleted values in the columns HomeDirectory and ProfilePath of an Active Directory user accounts cannot be provisioned. | 30561 |
| Error calculating Active Directory group memberships if the user account's primary group has been changed. | 30826 |
| Error synchronizing the Active Directory user account schema properties ObjectKeyManager and Secretary. Synchronization quits although the option Continue on error is set. | 30967 |
| Timeout during synchronization of Azure Active Directory group memberships. | 31051 |
| Global catalogs should be initialized when the first necessary access is made and not whilst establishing the connection to Active Directory. | 31178 |
| Not all permissions are documented that are required for synchronizing Microsoft Exchange. | 29901 |
| If a Microsoft Exchange address list is marked as outstanding, the associated address book entries are not marked as outstanding. | 30400 |
| Error deleting outstanding Microsoft Exchange address book entries. | 30401 |
| If a Microsoft Exchange mailbox database is marked as outstanding, its server assignments are not marked as outstanding. | 30466 |
| Error provisioning deleted Microsoft Exchange mailboxes if deferred deletion is | 30807 |

| Resolved issue | Issue ID |
|---|-----------------|
| configured. | |
| Loading Microsoft Exchange data availability groups fails if all the servers involved are shut down. | 31131 |
| The processing method <code>MarkAsOutstanding</code> is missing in the synchronization step <code>RoleAssignmentPolicy</code> for Microsoft Exchange. A patch with the patch ID VPR#28815 is available for synchronization projects. | 28815 |
| Error provisioning Exchange Online mailboxes. A patch with the patch ID VPR#31269 is available for synchronization projects. | 31269 |
| The process for provisioning memberships in E-Business Suite authorizations are repeatedly inserted in the Job queue if the user account's ID (column <code>UserID</code>) is not set. | 30349 |
| Date values in script properties are not converted into language dependent format. A patch with the patch ID VPR#28962_EBS is available for synchronization projects. | 28962 |
| Error setting up synchronization with an LDAP directory if an <code>AttributeType</code> is returned in quotes in the server schema. | 30366, 30337 |
| Canonical names of LDAP objects are not formatted automatically if the synchronization type is changed from No synchronization to One Identity Manager . | 30398 |
| Error setting up synchronization with IBM Notes if the connection to the Domino server is tested. | 30427 |
| Synchronization quits if the <code>FullName</code> of a Notes document cannot be loaded. | 30691 |
| The person document of a new Notes user account does not appear in the address book's default view. | 30814 |
| Error synchronizing Notes templates. | 30907 |
| Error renaming a Notes user account if an organization unit is assigned to it. | 30953 |
| Error adding a group based SharePoint Online user account. A patch with the patch ID VPR#30729 is available for synchronization projects | 30729 |
| The processing method <code>MarkAsOutstanding</code> is missing in a number of synchronization steps for SAP R/3 authorization objects. A patch with the patch ID VPR#29477 is available for synchronization projects. | 29477 |
| One Identity Manager Administration Guide for the SAP R/3 Compliance Add-on is missing a note informing the user that synchronization of SAP author- | 29676 |

| Resolved issue | Issue ID |
|--|-----------------|
| ization objects for central user administration clients is not supported. | |
| The options Home address and Default address can be disabled although only an email address is assigned to the SAP user account. | 29700 |
| During synchronization of SAP group, role or profile assignments to SAP user accounts from a secondary system, the assignments are not saved in the One Identity Manager database. | 29848 |
| Incorrect synchronization of organization structure objects from an SAP HCM system (HR0rgUnit). | 30121 |
| When adding SAP user account with parameters, email addresses, telephone and fax numbers, distinguished names (such as SAPComPhone.DistinguishedName) are not formatted. | 30356 |
| Too many post-processing tasks are sent to the DBQueue if changes are made to SAP user accounts. | 30361 |
| The Insert event is not triggered for tasks in the HelperSAPUserInSAPRole table. | 30367 |
| SAP role assignments to SAP user accounts are provisioned, although the associated categories do not match. | 30386 |
| If several changes are made to an employee's central password in quick succession, by the Password Capture Agent for example, only the first change is made to the SAP user accounts. | 30420 |
| Company assignment of SAP user accounts is not provisioned in the target system. A patch with the patch ID VPR#30453 is available for synchronization projects | 30453 |
| If an existing SAP user account is given the manage level Full managed , the IT operating data for the SAP communications data (SAPComPhone, SAPComFax and SAPComSMTP) is not calculated. | 30515 |
| Error synchronizing company data (table Company). | 30557 |
| Error loading single objects for schema types that are provided by a schema extension file. | 30653, 30701 |
| Executable SAP transactions are not calculated correctly for SAP user accounts. | 30718 |
| Error calculating role assignments (table SAPUserInSAPRole). | 30797, 31149 |
| Error in provisioning if the option Set effective password in Manager for a user account with the type Service or System has been set. | 30952, 30956 |
| Wrong templates for columns SAPComPhone.PhoneNumber and | 31105 |

| Resolved issue | Issue ID |
|--|-----------------|
| SAPComFax.FaxNumber. | |
| Error converting Json data with the data type Integer or Float. | 30536 |
| Error deleting group memberships with the SCIM connector. | 30710 |
| Cloud application group memberships are incorrectly resolved if the schema property members~type does not contain a value. | 31187 |
| The connectors Microsoft Exchange, Exchange Online and Windows PowerShell only use one revision counter even if several schema properties per schema type are flagged as revision counters. In synchronization projects that use the Windows PowerShell Connector, the target system schema must be reloaded to use more revision counters. A patch with the patch ID VPR#31026 is provided for Microsoft Exchange and Exchange Online synchronization projects. | 31026 |
| An Out-Of-Memory exception occurs while determining managers for email users and email contacts in large Exchange Online systems. | 31087 |
| The native database connector does not delete group memberships in the target system if provisioning is carried out by an application server. | 30659 |
| During synchronization of the native database connector, objects are marked as changed although they have not been changed. | 30840 |
| Spaces in schema property names that are flagged as revision counters, are not masked in the native database connector. | 30901 |

Table 8: Identity and Access Governance

| Resolved issue | Issue ID |
|---|-----------------|
| Attestations are discontinued with the reason "No approver available" even though an approver is available. | 30408 |
| Under certain circumstances, the Customizer method CreateAttestations blocks DBQueue processing. | 31016 |
| Error deleting attestation cases. | 31092 |
| Disabling attestation policies does not delete the associated attestation cases. | 31141 |
| In email notifications to attestors, the pictures defined in custom mail templates are not shown. | 31151 |
| Service items cannot be added as products in the IT Shop if their identifier is longer than 128 characters. | 30399 |
| In the approval sequence, the time is shown as UTC time. | 30483 |

| Resolved issue | Issue ID |
|--|-----------------|
| The script VI_BuildITShopLink_Unsubscribe creates a wrong link. | 30531 |
| Membership in a role cannot be delegated if the recipient of the delegation is already a member of this role. | 30549 |
| If a company resource is assigned by a limited period request and an unlimited period request at the same time and the limit period request expires, the company resource is removed although a valid, unlimited request still exists. | 30697 |
| The column templates ShoppingCartItem.ObjectKeyAssignment, DisplayObjectKeyAssignment and PersonWantsOrg.DisplayObjectKeyAssignment cannot be overwritten. | 30766 |
| Manager freezes when an approval workflow is copied. | 30833 |
| Initial login data is sent to the wrong employee when user accounts are requested in the IT Shop. | 31014 |
| Closed requests are not deleted, although the retention period must have expired. | 31068 |
| The DBQueue Processor checks automatic approval for requests that are already approved but not yet assigned (OrderState = 'Granted'). | 31076 |
| Incorrect testing of whether a company resource has already been assigned if the option Only for use in IT Shop is set. | 31116 |
| If an exception has been granted for a product with a rule violation in the approval process, the rule violation remains after the product has been canceled and the assignment removed. | 30213 |
| Ad-hoc rule checking does not create processing tasks for recalculating rule violations and for calculating the affected employee group. This means the affected employees may not be calculated correctly. | 30281 |
| If a disabled compliance rule is deleted, the associated rule violation is not deleted. | 30585 |
| Calculating rule violations also calculates disabled rules. | 30728 |
| Error calculating compliance after updating the One Identity Manager database if only modules that are not dependent on the Compliance Rules Module are selected. | 30905 |
| Wrong table name in One Identity Manager System Roles Administration Guide in section Disabled system roles . | 29226 |
| Error assigning an object from a custom table to a system role. | 30465 |
| As from version 7.1.2, company resource assignments of child system roles are not mapped in the table EsetHasEntitlement. However, by updating the One | 30614 |

| Resolved issue | Issue ID |
|---|-----------------|
| Identity Manager database to version 7.1.2 or later, assignments to child system roles are not removed from the table EsetHasEntitlement. | |
| System users with permissions groups vi_4_PERSONADMIN and VI_4_ALLMANAGER cannot add any employees. | 30052 |
| <p>i NOTE: By solving this issue, you may find that objects are not inserted properly because columns permissions are missing on compulsory fields. Table permissions of the respective permissions group are taken into account during calculation of each column permission. Table permissions of different permissions groups are no longer transferred to all columns. This means, a column cannot be edited when an object is inserted if the table permission Insertable is not defined for the permissions group that grants the column permission Editable.</p> | |
| In Manager, the Change security question task can also be displayed even though the logged in user does not have the required permissions. | 30287 |
| In the Show Entitlements Origin report, SAP roles and BI analysis authorizations that are inherited through system roles are missing. | 30291 |
| Error displaying the Employee Access Overview at specific point in time report. | 30859 |
| Display errors in the Filter Designer <ul style="list-style-type: none"> • Creating dynamic roles with many filter criteria • Select several elements from a menu | 29639, 30668 |
| If a simple report is generated in CSV format, an empty report is created. | 31073 |

See also:

- [Schema changes](#) on page 45
- [Patches for synchronization projects](#) on page 54

Known issues

The following is a list of issues known to exist at the time of release of One Identity Manager.

Table 9: General known issues

| Known Issue | Issue ID |
|--|--------------|
| If you connect to a database with the Database Compiler, the task QBM-K-CommonWaitForCompiler is immediately queued in the DBQueue. If the Database Compiler ends without compiling the database, the task remains in the DBQueue. | 23049, 24713 |
| Error in the Report Editor if columns are used that are defined in the Report Editor as keywords. Workaround: Create the data query as an SQL query and use aliases for the affected columns. | 23521 |
| Errors may occur if the Web Installer is started in several instances at the same time. | 24198 |
| Headers in reports saved as CSV do not contain corresponding names. | 24657 |
| In certain circumstances, objects can be in an inconsistent state after simulation in Manager. If an object is changed or saved during simulation and the simulation is finished, the object remains in the final simulated state. It may not be possible to save other modifications to this object instance. Solution: Reload the object after completing simulation. | 12753 |
| 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 |
| Schema extensions on a database view of type View (for example Department) with a foreign key relation to a base table column (for example BaseTree) or a database view of type View are not permitted. | 27203 |
| Error connecting through an application server or the API 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 |
| If a One Identity Manager database is operating in a cluster, the database is restored from a backup after a cluster failover. A new database ID is created in the process. This step cannot be missed out anymore otherwise the database cannot be compiled. | 28373 |
| It is not possible to extend predefined dynamic foreign keys by references to redefined tables. If you define custom dynamic foreign keys, at least one of the parties involved - dynamic foreign key column or referenced table - must | 29227 |

be a custom object.

Error resolving events on a view that does not have a UID column as a primary key. 29535

Primary keys for objects in the One Identity Manager always consist of one, or in the case of M:N tables, two UID columns. This is basic functionality in the system.

The definition of a view that uses the XObjectKey as primary key, is not permitted and would result in more errors in a lot of other places.

The consistency check **Table of type U or R with wrong PK definition** is provided for testing the schema.

The default setting of globallog.config assumes that write access exists for %localappdata%. If an EXE does not have sufficient permissions, the log can be written to a directory that does have the access rights by changing the variable logBaseDir in the globallog.config or by introducing a special log configuration in the *.exe.config or the Web.config file. 30048

The One Identity Manager Service only logs messages in the event log **Application**, by default. 30540

Cause: To add an event log with another name, you require administrator permissions on the Job server.

Solution:

1. Add the file that the One Identity Manager Service should write to manually on the Job server. You can use Windows PowerShell, for example, to do this.
 - a. Run Windows PowerShell as administrator on the Job server.
 - b. Run the following CmdLet:


```
New-EventLog -Source "Foobar" -LogName "<file name>"
```
2. Enter this file name in the One Identity Manager Service's configuration file as the name for the event log in the module Logwriter .
3. Restart the computer.
4. Restart the One Identity Manager Service.

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. The error, in case a Save Transaction is carried out is: Cannot use SAVE TRANSACTION within a distributed transaction. 30972

Solution: Disable the option DTC_SUPPORT = PER_DB.

Table 10: Web applications

| Known Issue | Issue ID |
|--|----------|
| <p>The error message This access control list is not in canonical form and therefore cannot be modified sometime occurs when installing the Web Portal with the Web Installer. The error occurs frequently after a Windows 10 Anniversary Update.</p> <p>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.</p> | 26739 |

Table 11: Target system connection

| Known Issue | Issue ID |
|--|----------|
| <p>Memory leaks occur with Windows PowerShell connections, which use Import-PSSession internally.</p> <hr/> <p>After synchronizing an SAP R/3 environment, assignments of single role to SAP user accounts are labeled as outstanding.</p> <p>This problem can occur if:</p> <ul style="list-style-type: none"> • SAP role assignments to user accounts were loaded in the One Identity Manager database before installing One Identity Manager 7.0.1 • Single role assignments, which are included in collective roles, were mapped as direct assignments (Error ID 3218196) <p>By resolving this problem in One Identity Manager 7.0.1, incorrect assignments are labeled as outstanding after synchronizing again using the appropriate synchronization configuration.</p> <p>Solution: Delete outstanding assignments in One Identity Manager target system synchronization.</p> | 23795 |
| <p>By default, the building block HR_ENTRY_DATE of an SAP HCM system cannot be called remotely.</p> <p>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.</p> | 25401 |
| <p>Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses were stored up to now.</p> | 27042 |
| <p>The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3.</p> <p>If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration.</p> | 27359 |

| Known Issue | Issue ID |
|---|----------|
| <ul style="list-style-type: none"> • 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. | |
| <p>No passwords can be provisioned when the bind method Fast Bind is in use in Active Directory. The SetPassword method is therefore not available.</p> <p>The process step AdhocProjection fails with the message:</p> <p>[System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKNOWNNAME)).</p> | 27427 |
| <p>Synchronization projects for SAP R/3 that were imported by a transport into a One Identity Manager database, cannot be opened. The problem only occurs if an SAP R/3 synchronization project was not added in the target database before importing the transport package.</p> <p>Solution: Create and save at least one SAP R/3 synchronization project before you import SAP R/3 synchronization projects into this database with the Database Transporter.</p> | 27687 |
| <p>Error in IBM Notes connector (Error getting revision of schema type ((Server))).</p> <p>Probable cause: The IBM Notes environment was rebuilt or numerous entries have been made in the Domino Directory.</p> <p>Solution: Update the Domino Directory indexes manually in the IBM Notes environment.</p> | 27126 |
| <p>Error provisioning licenses in a central user administration's child system.</p> <p>Message: No company is assigned.</p> <p>Cause: No company name could be found for the user account.</p> <p>Solution: Ensure that either:</p> <ul style="list-style-type: none"> • A company, which exists in the central system, is assigned to user account. - OR - • A company is assigned to the central system. | 29253 |
| <p>Error loading single objects with Windows PowerShell if the parameter Identity is used. The error can occur during provisioning of changes made to objects in Microsoft Exchange or Exchange Online, for example, and causes follow-on errors.</p> <p>Windows PowerShell connector's message: Command yielded <count> objects but only one was expected.</p> | 29152 |

| Known Issue | Issue ID |
|---|------------------|
| Cause: Multiple objects with the same name exist. | |
| Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will not come into effect until later. | 29556 |
| Cause: The function BAPI_EMPLOYEE_GETDATA is always executed with the current date. Therefore, changes are taken into account on a the exact day. | |
| Solution: To synchronize personnel data in advance that will not come into effect later, use a schema extension and load the data from the table PA0001 directly. | |
| Error synchronizing an OpenDJ system, if a password begins with an open curly bracket. | 29620 |
| Cause: The LDAP server interprets a generated password of the form {<abc>}<def> as a hash value. However, the LDAP server does not allow hashed passwords to be passed. | |
| Solution: The LDAP server can be configured so that a hashed password of the form {<algorithm>}hash can be passed. | |
| <ul style="list-style-type: none"> • On the LDAP server: Allow already hashed passwords to be passed. • In the synchronization project: Only pass hashed passwords. Use the script properties for mapping schema properties that contain passwords. Create the password's hash value in the script. | |
| Target system synchronization does not show any information in the Manager web application. | 30271 |
| Workaround: Use Manager to run the target system synchronization. | |
| 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 : | 796028, 30963 |
| 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. | |
| The following error message is displayed while setting up a synchronization project for One Identity Safeguard: | 31048 |
| 404: Not Found -- 0: | |
| Cause: An older One Identity Safeguard version that does not support One Identity Manager is in use. | |
| Solution: Ensure that you are using One Identity Safeguard version 2.5. | |
| Inconsistencies in SharePoint can cause errors by simply accessing a property. | 31017 |

| Known Issue | Issue ID |
|-------------|----------|
|-------------|----------|

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.

Table 12: Third party contributions

| Known Issue | Issue ID |
|--|-----------------------------|
| An error can occur during synchronization of SharePoint websites under SharePoint 2010. The method SPWeb.FirstUniqueRoleDefinitionWeb() triggers a ArgumentException. For more information, see https://support.microsoft.com/en-us/kb/2863929 . | 24626 |
| 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-Komponente 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: <ul style="list-style-type: none"> • Windows Server 2016 : KB4462928 • Windows Server 2012 R2 : KB4462926, KB4462921 • Windows Server 2008 R2 : KB4462926 | 30575 |

We do 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 groups during provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem.

Schema changes

The following provides an overview of schema changes from One Identity Manager version 8.0.2 up to version 8.1.

Configuration Module

- New column `DialogColumn.CanEditScript` for scripts to conditionally remove edit permissions from columns.
- New column `DialogColumn.CanSeeScript` for scripts to conditionally remove viewing permissions from columns.
- New column `DialogColumn.IsElementProperty` to flag columns as name components for password validation.
- New column `DialogConfigParm.UID_QBMC1rTypeEditor` to embed an editor for editing more complex configuration parameters.
- New column `DialogDatabase.LicenceID` for flagging license information.
- New column `DialogDatabase.ProductionLevelAddOn` (in progress).
- New column `DialogAEDSAction.IsInactive` to disable individual objects.
- New columns `DialogReportQuery.HAssignFKColumn`, `DialogReportQuery.HAssignType`, `DialogReportQuery.HListColumns` and `DialogReportQuery.HObjColumns` for queries for reports with historical data.
- New column `DialogTag.SortOrder` as sort order for change labels.
- New columns `DialogTree.ListActivationFKList` and `DialogTree.NodeActivationFKList` for navigating to a foreign key object, which is loaded when an entry is selected in the user interface.
- New column `DialogUser.IsLockedOut` for specifying whether a user is blocked due to failed logins.
- New column `DialogValidDynamicRef.IsForAddElementAffected` and `QBMRRelation.IsForAddElementAffected` for flagging whether the parent object in the Job queue is added.
- New columns `Job.IsNoDBQueueDefer`, `JobQueue.IsNoDBQueueDefer` and

JobTask.IsNoDBQueueDefer for flagging whether process handling waits until DBQueue Processor tasks have been handled.

- New column QBMDBQueueSlot.XObjectKey.
- New column QBMServer.IsInitQueueRunning flags whether the Job queue is initialized.
- New columns QBMPwdPolicy.IsLowerLetterNotAllowed, QBMPwdPolicy.IsNumberNotAllowed, QBMPwdPolicy.IsSpecialNotAllowed and QBMPwdPolicy.IsUpperLetterNotAllowed for password policies.
- New column QBMServer.LastJobFetchTime for last time the process was called.
- New column QBMServer.PortNumber as port for displaying the One Identity Manager Service log in a browser.
- New columns QBMVSystemOverview.QualityOfValue and QBMVSystemOverview.RecommendedValue for showing system configuration in a report.
- New column QBMWebApplication.UID_QBMIdentityClient for allocating a OAuth 2.0/OpenID Connect configuration to a web application.
- New table DialogGroupHasAEDS for mapping API file permissions.
- New table DialogGroupInProductLimited for mapping permissions groups to applications.
- New table DialogObjectHasMethod for assigning task definitions to objects definitions.
- New tables QBMDBPrincipal, QBMDBRoleDef, QBMDBPrincipalHasRoleDef and QBMDBRightsAddOn for mapping granulated permissions to SQL Server and database levels.
- New table QBMDBQueueTaskPerf for analyzing the DBQueue Processor task performance.
- New tables QBMDDevBranch and QBMDDevBranchHasAssembly for version management of API projects.
- New table QBMHtmlApp for maintaining information about HTML applications.
- New tables QBMIdentityClient, QBMIdentityProvider, QBMIdentityProvDisabledCol and QBMIdentityProvEnabledCol for OAuth 2.0/OpenID Connect configuration.
- New table QBMLaunchActionHasFeature for authorizing Launchpad actions through program functions.
- New table QBMReportQueryCriteria for defining several criteria for historical reports.
- New table QBMVNonUniqueMAllTable for listing tables without a unique combination of object and foreign key (for optimizing index generating).
- The following tables have been deleted:
 - DialogValidParent
 - QBMPermissionSettingBase
- The following columns have been deleted:
 - DialogDatabase.IsFullTextEnabled

DialogMethod.UID_DialogObject
DialogReportQuery.HListCriteriaColumn
DialogReportQuery.HListCriteriaValue
QBMWebApplication.CertificateEndpoint
QBMWebApplication.CertificateText
QBMWebApplication.OAuthCertificateSubject
QBMWebApplication.OAuthCertificateThumbPrint
QBMWebApplication.OAuthResource
QBMWebApplication.SharedSecret

Target System Synchronization Module

- New column DPRNameSpaceHasDialogTable.RootObjectPath as path to the base object.
- New column DPRProjectionConfig.LogVariableSetContents flags whether variable sets are logged with current values.
- New columns DPRProjectionConfigStep.CommitPropertiesLeft, DPRProjectionConfigStep.CommitPropertiesMode and DPRProjectionConfigStep.CommitPropertiesRight for improving object based synchronization.
- New column DPRSchemaMethod.MethodType for flagging processing methods.
- New columns DPRShell.EditedBy and DPRShell.EditedSince for flagging whether a synchronization project is already being processed.
- New columns DPRShell.ShadowCopy and DPRShell.ShadowCopyMode for optimizing how synchronization projects are loaded.
- New column DPRSystemConnection.DisplayNameQualified as qualified display name for the system connection.
- New column DPRTemplate.SortOrder for sorting project templates.
- New table DPRScript as script library.
- New tables DPRStartSequence and DPRStartSequenceHasProjection for managing the start order.

Target System Base Module

- New mandatory field definition for the following columns:
 - TSBAccountDef.ObjectKeyTargetSystem
 - TSBITData.ObjectKeyAppliesTo
- The table TSBVGroupTable has been deleted.
- The column UNSRoot.isMemberOfEnabled has been deleted.

Active Directory Module

- New column ADSAccount.MSDsConsistencyGuid as reference to the Cloud user account.
- New column ADSSite.UID_ADSEForest as reference to the forest.
- New mandatory field definition for the following columns:
 - ADSContainer.UID_ADSEDomain
 - ADSPolicy.UID_ADSEDomain
 - ADSPrinter.UID_ADSEMachine
 - ADSEDomain.UID_ADSEForest
- The column ADSSite.UID_ADSEDomain has been deleted.

Microsoft Exchange Module

- New column EX0RoleAssignPolicy.XMarkedForDeletion for flagging whether a policy is marked for deletion or not.
- New mandatory field definition for the following columns:
 - EX0ActiveSyncMBPolicy.UID_EX0Organization
 - EX0AddrList.UID_EX0Organization
 - EX0DAG.UID_EX0Organization
 - EX0DL.UID_EX0Organization
 - EX0DynDL.UID_EX0Organization
 - EX0MailBox.UID_EX0Organization
 - EX0MailBoxDatabase.UID_EX0Organization
 - EX0MailContact.UID_EX0Organization
 - EX0MailPublicFolder.UID_EX0Organization
 - EX0MailUser.UID_EX0Organization
 - EX0ManagedFolderPolicy.UID_EX0Organization
 - EX0OfflAddrBook.UID_EX0Organization
 - EX0PublicFolder.UID_EX0Organization
 - EX0PublicFolderDatabase.UID_EX0Organization
 - EX0RetentionPolicy.UID_EX0Organization
 - EX0RoleAssignPolicy.UID_EX0Organization
 - EX0Server.UID_EX0Organization

Exchange Hybrid Module

- New column EXHRemoteMailbox.EmailAddresses for mapping more email addresses to other email addresses for remote mailboxes.

- New column EXHRemoteMailbox.EmailAddressPolicyEnabled for specifying whether the email address is automatically updated on the basis of the recipient policy.
- New mandatory field definition for the column EXHRemoteMailbox.UID_EX00Organization.

IBM Notes Module

- New mandatory field definition for the following columns:

NDOAdmin4.UID_NDODomain
 NDOCertifier.UID_NDODomain
 NDOCertifierRequest.UID_NDODomain
 NDOGroup.UID_NDODomain
 NDOMailInDB.UID_NDODomain
 NDOServer.UID_NDODomain
 NDOUser.UID_NDODomain

LDAP Module

- New mandatory field definition for the column LDAPContainer.UID_LDPDomain.

Oracle E-Business Suite Module

- New mandatory field definition for the following columns:

EBSApplication.UID_EBSSystem
 EBSDataGroup.UID_EBSSystem
 EBSMenu.UID_EBSSystem
 EBSResp.UID_EBSSystem
 EBSSecurityGroup.UID_EBSSystem
 EBSUser.UID_EBSSystem

SharePoint Module

- New columns SPSGroupPermission.XMarkedForDeletion and SPSUserPermission.XMarkedForDeletion for flagging whether permissions are marked for deletion.
- New mandatory field definition for the following columns:
 - SPSLanguage.UID_SPSFarm
 - SPSWebApplication.UID_SPSFarm
 - SPSSite.UID_SPSWebApplication

SAP R/3 User Management module Module

- New column `SAPUserHasParameter.ParameterValueDirect` for finding parameter values assigned directly in the target system.
- New column `SAPUserInSAPRole.DisplayValue` as display name for memberships.
- New tables `SAPBaseTreeHasParameter`, `DepartmentHasSAPPParameter`, `LocalityHasSAPPParameter`, `OrgHasSAPPParameter` and `ProfitCenterHasSAPPParameter` for assigning SAP parameters to company structures.
- New table `SAPUserMandant` for mapping access permissions to CUA systems.
- New mandatory field definition for the following columns:
 - `SAPProfitCenter.UID_SAPMandant`
 - `SAPMandant.UID_SAPSystem`
 - `SAPLoginLanguages.UID_SAPSystem`
- The table `SAPUserInSAPMandant` has been deleted.

SAP R/3 Compliance Add-on Module

- New column `XMarkedForDeletion` in tables `SAPAuthObjectClass`, `SAPBaseTreeInSAPFunction`, `SAPFieldHasSAPRCTable`, `SAPFunctionInstanceDetail`, `SAPRCTable`, `SAPRCVariable`, `SAPTransactionHasSAPAuthObject` and `SAPUserInSAPFunction` for flagging whether the objects are marked for deletion.
- New mandatory field definition for the following columns:
 - `SAPAuthObject.UID_SAPSystem`
 - `SAPAuthObjectClass.UID_SAPSystem`
 - `SAPVariableSet.UID_SAPMandant`

Privileged Account Governance Module

- New data model for the Privileged Account Governance Module.

Identity Management Base Module

- New columns `AERole.UID_PersonHead` and `AERole.UID_PersonHeadSecond` for mapping managers for application roles.
- New column `Person.ContactEmail` as contact email address for the self-registration portal.
- New column `Person.EmployeeType` for mapping employee types.
- New column `Person.IsLockedOut` for specifying whether employee is blocked due to failed logins.
- New column `Person.IsLockedPwdAnswer` for specifying whether the dialog box for changing the password is blocked due to failed logins.
- New column `Person.UID_DialogCultureFormat` for specifying the language for

displaying language specific numbers and dates in the Web Portal user interface.

- New columns `PersonWantsOrg.CheckResult`, `PersonWantsOrg.CheckResultDetail`, `ShoppingCartItem.CheckResult`, `ShoppingCartItem.CheckResultDetail` and `ShoppingCartOrder.CheckStatus` for asynchronous processing of requests.
- New columns `PWODecisionMethod.UID_DialogRichMailProlongate` and `PWODecisionMethod.UID_DialogRichMailUnsubscribe` for specifying other mail templates in approval policies.
- New column `QERJustification.JustificationType` for specifying a usage type for standard reasons.
- New table `BaseTreeOwnsObject` for finding target system managers quicker.
- New table `QEROrgRootHasOrgType` for defining role types for role classes.
- New table `QERPasswordQueryAndAnswer` for password questions and answers for resetting passwords.
- New table `QERVPersonCentralPwdColumn` for defining user account properties that employees' central passwords are mapped to.
- The following columns have been extended from `nvarchar(128)` to `nvarchar(256)`:
 - `AERole.Ident_AERole`
 - `BaseTree.Ident_Org`
 - `DelegableItem.DisplayValue`
 - `QERVDelegableItem.DisplayValue`
 - `Department.DepartmentName`
 - `ITShopOrg.Ident_Org`
 - `ITShopSrc.Ident_Org`
 - `Locality.Ident_Locality`
 - `PersonWantsOrg.DisplayOrg`
 - `PersonWantsOrg.DisplayOrgParent`
 - `PersonWantsOrg.DisplayOrgParentOfParent`
 - `ProfitCenter.ShortName`
 - `ShoppingCartItem.DisplayOrg`
- The following columns have been deleted:
 - `Person.PasswordAnswer`
 - `Person.PasswordQuery`

Business Roles Module

- Column `Org.Ident_Org` extended from `nvarchar(128)` to `nvarchar(256)`.

Attestation Module

- New column `AttestationHelper.UID_PWORulerOrigin` for determining the attester.

Compliance Rules Module

- Column `NonCompliance.Ident_NonCompliance` extended from `nvarchar(128)` to `nvarchar(256)`.

Helpdesk Module

- New column `HDSSupporterGroup.XMarkedForDeletion` for flagging whether a support team is marked for deletion.

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 8.0.2 to version 8.1. Apply the patches to existing synchronization projects. For more information, see [Applying patches to synchronization projects](#) on page 73.

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 54.

Table 13: Overview of synchronization templates and patches

| Module | Synchronization template | Type of modification |
|---------------------------------|--|----------------------|
| Azure Active Directory Module | Azure Active Directory synchronization | none |
| 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 synchronization | none |
| Oracle E-Business Suite Module | Oracle E-Business Suite synchronon- | changed |

| Module | Synchronization template | Type of modification |
|---|--|-----------------------------|
| | ization | |
| | Oracle E-Business Suite CRM data | changed |
| | Oracle E-Business Suite HR data | changed |
| | Oracle E-Business Suite OIM data | changed |
| Microsoft Exchange Module | Microsoft Exchange 2010 synchronization (deprecated) | none |
| | Microsoft Exchange 2010 synchronization (deprecated) | none |
| | Microsoft Exchange 2010 synchronization (v2) | changed |
| | Microsoft Exchange 2013_2016 synchronization (v2) | changed |
| G Suite Module | G Suite synchronization | changed |
| LDAP Module | AD LDS Synchronization | None |
| | OpenDJ Synchronization | none |
| IBM Notes Module | Lotus Domino synchronization | changed |
| Exchange Online Module | Exchange Online synchronization (deprecated) | changed |
| | Exchange Online synchronization (v2) | changed |
| Privileged Account Governance Module | One Identity Safeguard synchronization | new |
| SAP R/3 User Management module Module | SAP R/3 Synchronization (Base Administration) | changed |
| | 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 |

| Module | Synchronization template | Type of modification |
|----------------------------------|--|----------------------|
| SharePoint Online Module | SharePoint Online synchronization | none |
| Universal Cloud Interface Module | SCIM Connect via One Identity Starling Connect | changed |
| | SCIM synchronization | changed |
| Unix Based Target Systems Module | Unix Account Management | none |
| | AIX Account Management | none |

Patches for synchronization projects

Patches for the following patch types are provided in One Identity Manager 8.1.

- Patches for solved issues
- Patches for new functions
- Milestones

To adjust existing synchronization projects to One Identity Manager version 8.1, you must implement milestones. A milestone is provided for each context. A milestone includes all patches for solved 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 8.1.

Patches for new functions can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 8.1 for synchronization projects. Only patches created after version 8.0.2. 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 functions.

For more information, see [Applying patches to synchronization projects](#) on page 73.

Table 14: General patches

| Patch ID | Patch | Description | Issue ID |
|---------------|-------|---|----------|
| Milestone 8.1 | | Milestone for the context DPR . | |
| Milestone 8.1 | | Milestone for the context One Identity Manager . | |

Table 15: Patches for Azure Active Directory

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|---|----------|
| | Milestone 8.1 | Milestone for the context Azure Active Directory . | |

Table 16: Patches for Active Directory

| Patch ID | Patch | Description | Issue ID |
|-------------|---|---|----------|
| VPR#29087 | Add the schema property mS-DS-ConsistencyGuid | Adds the schema property mS-DS-ConsistencyGuid in the User and InetOrgPerson maps. | 29087 |
| VPR#29306 | Schema class ADSSite (all) (part 1) correction | Changes the foreign key for ADSSite from ADSDomain to ADSFroest. Prerequisite for patch Schema class ADSSite (all) (part 2) correction . This patch is applied during the One Identity Manager automatic update. | 29306 |
| VPR#29306_2 | Schema class ADSSite (all) (part 2) correction | Changes the foreign key for ADSSite from ADSDomain to ADSFroest. Dependent on patch Schema class ADSSite (all) (part 2) correction . This patch is applied during the One Identity Manager automatic update. | 29306 |
| VPR#30192 | Scope definition and usage of processing method MarkAsOutstanding | Adds a scope and the processing method MarkAsOutstanding to the synchronization step trustedDomain. | 30192 |
| | Milestone 8.1 | Milestone for the context Active Directory . | |

Table 17: Patches for Active Roles

| Patch ID | Patch | Description | Issue ID |
|-----------|---|---|----------|
| VPR#28612 | Adds new property mapping rules to the Computer mapping | Adds property mapping rules for OperatingSystem, OperatingSystemVersion and OperatingSystemServicePack to the Computer mapping. | 28612 |
| VPR#29087 | Add the schema property mS-DS- | Adds the schema property mS-DS-ConsistencyGuid in the User and | 29087 |

| Patch ID | Patch | Description | Issue ID |
|----------|-----------------|---|----------|
| | ConsistencyGuid | InetOrgPerson maps. | |
| | Milestone 8.1 | Milestone for the context Active Roles . | |

Table 18: Patches for Oracle E-Business Suite

| Patch ID | Patch | Description | Issue ID |
|-------------------|--|--|----------|
| VPR#28962_ EBS | Change date conversion in script properties | A language independent format is used for converting date values in script properties. This patch is applied during the One Identity Manager automatic update. | 28962 |
| VPR#29265 | Extended processing methods in the synchronization step HR PersonManager | Extended the synchronization configuration EBS_Person_RemoveManager in the synchronization step HR PersonManager. This patch is applied during the One Identity Manager automatic update. | 29265 |
| VPR#29741 | Extended synchronization configuration by HR PersonPrimaryLocation | Extends a synchronization step and a mapping for synchronizing employees' primary locations. | 29741 |
| VPR#30464 | Support for Oracle Database Editions | Adds a variable to the Oracle Database Edition configuration. | 30464 |
| VPR#31011 | Change serialization format | Changes the serialization format of the schema types and reloaded the target system schema. This patch is applied during the One Identity Manager automatic update. | 31011 |
| | Milestone 8.1 | Milestone for the context Oracle E-Business Suite . | |

Table 19: Patches for Microsoft Exchange

| Patch ID | Patch | Description | Issue ID |
|-----------|--|---|----------|
| VPR#28815 | Extends a processing method in the synchronization step RoleAssignmentPolicy | Extends the processing method MarkAsOutstanding in the synchronization step RoleAssignmentPolicy. | 28815 |

| Patch ID | Patch | Description | Issue ID |
|-----------|------------------------------|---|----------|
| VPR#31026 | Optimizes revision filtering | Reloads the target system schema and replaces the revision counters whenChangedUTC and whenCreatedUTC with vrtRevision. | 31026 |
| | Milestone 8.1 | Milestone for the context Microsoft Exchange . | |

Table 20: Patches for Exchange Online

| Patch ID | Patch | Description | Issue ID |
|-----------|---|---|----------|
| VPR#30498 | Removes property mapping rules from the OwaMailboxPolicy mapping | Removes property mapping rules BoxAttachmentsEnabled, DropboxAttachmentsEnabled and GoogleDriveAttachmentsEnabled from the OwaMailboxPolicy mapping. | 30498 |
| VPR#30588 | Extends schema properties and property mapping rules in Calendar Processing (User/Shared) and Calendar Processing (Resource) mappings | Extends member lists in the schema properties vrtBookInPolicy, vrtRequestInPolicy and vrtRequestOutOfPolicy and updates the property mapping rules accordingly. | 30588 |
| VPR#31026 | Optimizes revision filtering | Reloads the target system schema and replaces the revision counters whenChangedUTC and whenCreatedUTC with vrtRevision. | 31026 |
| VPR#31269 | Modified implementation by extending various property mapping rules by a condition. | In the Mailbox mapping, a condition was added to various property mapping rules to modify implementation. | 31269 |
| | Milestone 8.1 | Milestone for the context Exchange Online . | |

Table 21: Patches for G Suite

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|--|----------|
| | Milestone 8.1 | Milestone for the context G Suite . | |

Table 22: Patches for LDAP

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|---|----------|
| | Milestone 8.1 | Milestone for the context LDAP . | |

Table 23: Patches for IBM Notes

| Patch ID | Patch | Description | Issue ID |
|-----------|--|---|----------|
| VPR#30313 | Mapping for mailbox file access levels | Inserts a property mapping rule for access levels of mailbox files in the Person mapping. | 30313 |
| | Milestone 8.1 | Milestone for the context IBM Notes . | |

Table 24: Patches for SAP R/3

| Patch ID | Patch | Description | Issue ID |
|-------------|---|--|----------|
| VPR#28147 | Deletes the mapping userInMandant | Deletes the mapping userInMandant. The map is replaced by userMandant. Prerequisite for patch New mapping userMandant . This patch is applied during the One Identity Manager automatic update. | 28147 |
| VPR#28147_2 | New mapping userMandant | New mapping for accessing client user accounts (userMandant). Depends on patch Deletes the mapping userInMandant . This patch is applied during the One Identity Manager automatic update. | 28147 |
| VPR#30453 | New property mapping rule for provisioning company data | New property mapping rule for mapping user account for provisioning company data. This patch is applied during the One Identity Manager automatic update. | 30453 |
| VPR#30941 | Blacklist rule filter on "userInCUARole" step | Defines property mapping rules to be excluded from the provisioning workflow's process step userInCUARole. This patch is applied during the One Identity Manager automatic update. | 30941 |
| | Milestone 8.1 | Milestone for the context SAP R/3 . | |

Table 25: Patches for SAP R/3 personnel planning data and structural profiles

| Patch ID | Patch | Description | Issue ID |
|-----------|--|---|----------|
| VPR#29265 | Extends a processing method in the synchronization step Managers | Extended the processing method SHR_Department_RemoveManager in the synchronization step Managers This patch is applied during the One Identity Manager automatic update. | 29265 |
| | Milestone 8.1 | Milestone for the context SAP R/3 structural profile add-on. | |

Table 26: Patches for SAP R/3 BI analysis authorizations

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|--|----------|
| | Milestone 8.1 | Milestone for the context SAP R/3 analysis authorizations add-on. | |

Table 27: Patches for SAP R/3 authorization objects

| Patch ID | Patch | Description | Issue ID |
|-----------|---|--|----------|
| VPR#29477 | Applies the processing method MarkAsOutstanding | Applies the processing method MarkAsOutstanding in various synchronization step. | 29477 |
| | Milestone 8.1 | Milestone for the context SAP R/3. | |

Table 28: Patches for SharePoint

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|--|----------|
| | Milestone 8.1 | Milestone for the context SharePoint. | |

Table 29: Patches for SharePoint Online

| Patch ID | Patch | Description | Issue ID |
|-----------|--|---|----------|
| VPR#30729 | Corrects property Mandatory property of SharePoint Online User.LoginName. | Changes property Mandatory of schema property LoginName of schema class User (all). This patch is applied during the One Identity Manager automatic update. | 30729 |
| | Milestone 8.1 | Milestone for the context SharePoint Online. | |

Table 30: Patches for the SCIM interface (in Universal Cloud Interface Module)

| Patch ID | Patch | Description | Issue ID |
|-----------|-------------------------------------|--|----------|
| VPR#30497 | Allows configuration of local cache | Adds a variable for disabling use of local cache. This patch is applied during the One Identity Manager automatic update. | 30497 |
| | Milestone 8.1 | Milestone for the context SCIM . | |

Table 31: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|--|----------|
| | Milestone 8.1 | Milestone for the context Universal Cloud Interface . | |

Table 32: Patches for Unix

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|---|----------|
| | Milestone 8.1 | Milestone for the context Unix . | |

Table 33: Patches for the One Identity Manager connector

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|---|----------|
| | Milestone 8.1 | Milestone for the context Database . | |

Table 34: Patches for the CSV connector

| Patch ID | Patch | Description | Issue ID |
|----------|---------------|--|----------|
| | Milestone 8.1 | Milestone for the context CSV . | |

Deprecated features

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

- Oracle Database is no longer supported as a database system for the One Identity Manager database.

NOTE: Oracle Data Migrator is provided to help you convert the database system. The Oracle Data Migrator takes all the data belonging to an Oracle Database's database user from version 8.0.1 or later and transfers it to an SQL Server database with the same version.

You can obtain the tool and a quick guide from the support portal. To access the Support Portal, go to <https://support.oneidentity.com/identity-manager/>.

- The process component SvnComponent has been removed.
- Google ReCAPTCHA Version 1 is no longer supported.

The following functions will be discontinued in later One Identity Manager versions and should no longer be utilized:

- In future, mutual aid as well as password questions and answers will not be supported in the Manager.
Use the Password Reset Portal to change passwords. Save your passwords and questions in the Web Portal.
- In future, the configuration parameter **QER | Person | UseCentralPassword | PermanentStore** will not be supported and will be deleted.
- In future, the table OS will not be supported and will be removed from the One Identity Manager schema.

System requirements

Ensure that your system meets the following minimum hardware and system requirements before installing One Identity Manager. For more detailed information about system prerequisites, see the *One Identity Manager Installation Guide*.

Minimum requirements for the database server

| | |
|--------------------|---|
| Processor | 8 physical cores 2.5 GHz+ |
| | NOTE: 16 physical cores are recommended on the grounds of performance. |
| Memory | 16 GB+ RAM |
| Hard drive storage | 100 GB |
| Operating | Windows operating system |

| | |
|----------|--|
| system | <ul style="list-style-type: none"> Note the requirements from Microsoft for the SQL Server version installed. <p>UNIX and Linux operating systems</p> <ul style="list-style-type: none"> Note the minimum requirements given by the operating system manufacturer for SQL Server databases. |
| Software | <p>Following versions are supported:</p> <ul style="list-style-type: none"> SQL Server 2017 Standard Edition (64-bit) with the current cumulative update SQL Server 2016 Standard Edition (64-bit), Service Pack 2 with the current cumulative update Compatibility level for databases: SQL Server 2016 (130) Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) <p>NOTE: The SQL Server Enterprise Edition is strongly recommended on performance grounds.</p> |

Minimum requirements for the service server

| | |
|--------------------|--|
| Processor | 8 physical cores 2.5 GHz+ |
| Memory | 16 GB RAM |
| Hard drive storage | 40 GB |
| Operating system | <p>Windows operating system</p> <p>Following versions are supported:</p> <ul style="list-style-type: none"> Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later <p>Linux operating system</p> <ul style="list-style-type: none"> Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. |
| Additional | Windows operating system |

software

- Microsoft .NET Framework Version 4.7.2 or later

i **NOTE:** Take the target system manufacturer's recommendations for connecting the target system into account.

Linux operating system

- Mono 5.14 or later
-

Minimum requirements for clients

| | |
|---------------------|---|
| Processor | 4 physical cores 2.5 GHz+ |
| Memory | 4 GB+ RAM |
| Hard drive storage | 1 GB |
| Operating system | Windows operating system <ul style="list-style-type: none">• Windows 10 (32-bit or 64-bit) with version 1511 or later• Windows 8.1 (32-bit or 64-bit) with the current service pack• Windows 7 (32-bit or non-Itanium based 64-bit) with the current service pack |
| Additional software | <ul style="list-style-type: none">• Microsoft .NET Framework Version 4.7.2 or later |
| Supported browsers | <ul style="list-style-type: none">• Internet Explorer 11 or later• Firefox (Release Channel)• Chrome (Release Channel)• Microsoft Edge (Release Channel) |

Minimum requirements for the Web Server

| | |
|--------------------|----------------------------|
| Processor | 4 physical cores 1.65 GHz+ |
| Memory | 4 GB RAM |
| Hard drive storage | 40 GB |
| Operating | Windows operating system |

system

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later

Linux operating system

- 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 Windows operating system software

- Microsoft .NET Framework Version 4.7.2 or later
- Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and 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 5.14 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

| | |
|---------------------|--|
| Processor | 8 physical cores 2.5 GHz+ |
| Memory | 8 GB RAM |
| Hard drive storage | 40 GB |
| Operating system | <p>Windows operating system</p> <ul style="list-style-type: none">• Windows Server 2016• Windows Server 2012 R2• Windows Server 2012• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later <p>Linux operating system</p> <ul style="list-style-type: none">• 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 | <p>Windows operating system</p> <ul style="list-style-type: none">• Microsoft .NET Framework Version 4.7.2 or later• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and Role Services:<ul style="list-style-type: none">• 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 <p>Linux operating system</p> <ul style="list-style-type: none">• NTP - Client |

- Mono 5.14 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 35: 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. i 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 (String Representation of Distinguished Names) and RFC 4512 (Directory Information Models). i NOTE: Other schema and provisioning process adjustments can be made depending on the schema. |
| Web service connector | Any SOAP web service providing wsdl. i 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 2003 , Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016. |
| Microsoft | <ul style="list-style-type: none"> • Microsoft Exchange 2010 Service Pack 3 or later |

Connector Supported data systems

| | |
|------------------------------|---|
| Exchange connector | <ul style="list-style-type: none">• Microsoft Exchange 2013 Service Pack 1 or later• Microsoft Exchange 2016• Microsoft Exchange hybrid |
| SharePoint connector | <ul style="list-style-type: none">• SharePoint 2010• SharePoint 2013• SharePoint 2016 |
| SAP R/3 connector | <ul style="list-style-type: none">• SAP Web Application Server 6.40• SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40 SR 2, 7.41, 7.50• SAP ECC 5.0 and 6.0• SAP S/4HANA On-Premise-Edition |
| Unix connector | Supports the most common Unix and Linux derivatives. For more information, see the Authentication Services specifications. |
| IBM Notes connector | <ul style="list-style-type: none">• Lotus Domino Server Version 8.0 up to Lotus Domino Server Version 9.0• IBM Notes Client 8.5.3 is supported as client version. |
| Native database connector | <ul style="list-style-type: none">• SQL Server• Oracle Database• SQLite• MySQL• DB2 (LUW)• CData ADO.NET Provider• SAP HANA |
| Mainframe connector | <ul style="list-style-type: none">• RACF• IBM i• CA Top Secret• CA ACF2 |
| Windows PowerShell connector | <ul style="list-style-type: none">• Windows PowerShell version 3 or later |
| Active Roles connector | <ul style="list-style-type: none">• Active Roles 6.9, 7.0, 7.2 |

Connector Supported data systems

| | |
|-----------------------------------|--|
| Azure Active Directory connector | <ul style="list-style-type: none">• Microsoft Azure Active Directory |
| SCIM connector | Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0. |
| Exchange Online connector | <ul style="list-style-type: none">• Microsoft Exchange Online |
| G Suite Connector | <ul style="list-style-type: none">• G Suite |
| Oracle E-Business Suite connector | <ul style="list-style-type: none">• Oracle E-Business Suite System versions 12.1 and 12.2 |
| SharePoint Online connector | <ul style="list-style-type: none">• Microsoft SharePoint Online |
| One Identity Safeguard connector | <ul style="list-style-type: none">• One Identity Safeguard version 2.5 |

Product licensing

Use of this software is governed by the Software Transaction Agreement found at <http://www.oneidentity.com/legal/sta.aspx> and the SaaS Addendum at <http://www.oneidentity.com/legal/saas-addendum.aspx>. This software does not require an activation or license key to operate.

Upgrade and installation instructions

To install One Identity Manager 8.1 for the first time, follow the installation instructions in the *One Identity Manager Installation Guide*. For more detailed instructions about updating, see the *One Identity Manager Installation Guide*.

! **IMPORTANT:** Note the [Advice for updating One Identity Manager](#) on page 69.

Advice for updating One Identity Manager

- 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 8.1. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
 - Automatic software updating of version 7.0 to version 8.1 only works smoothly if the service pack 7.0.3 is installed. In addition, the files VI.Update.dll and JobService.dll must be installed.

Request the files VI.Update.dll and JobService.dll from the support portal.

To distribute the file, use the Software Loader.

Future service packs of 7.0 versions will already contain the changes to these files, and therefore, must not distributed separately.
 - Automatic software updating of version 7.1 to version 8.1 only works smoothly if the service pack 7.1.3 is installed.

- One Identity Manager uses In-Memory OLTP ((Online Transactional Processing) for memory optimized data access. 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 of a One Identity Manager database, different columns that were already semantically defined as mandatory fields become physical mandatory fields. For more information, see [Schema changes](#) on page 45.

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\Files\MSSQL2K\30374.sql) is provided. In case it fails, correct the data and restart the update.

- During installation of a new One Identity Manager database version 8.1 or while

updating a One Identity Manager database from version 7.0, 7.1 or 8.0 to version 8.1, 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*.

Adjust the configuration parameter after updating the One Identity Manager. 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.

If you want to change to granular permissions at a later date, contact support. To access the Support Portal, go to <https://support.oneidentity.com/identity-manager/>.

- To successfully compile HTML applications with the Configuration Wizard, you must download packages from the NPM repository. Ensure that the workstation running the Configuration Wizard can establish a connection to the website <https://registry.npmjs.org>.

Alternatively, it is possible to download the packages from a proxy server and make them available manually. For more information, see the knowledge article <https://support.oneidentity.com/kb/266000>.

- In One Identity Manager versions 8.0, 8.0.1, 8.0.2, the One Identity Manager History Service and the One Identity Manager Service were both installed when the One Identity Manager History Database was installed.

If you are affected by this problem, uninstall the One Identity Manager History Service before updating your One Identity Manager History Database. Run the following command as administrator:

```
sc delete "HDBService"
```

Updating One Identity Manager to version 8.1

IMPORTANT: Note the [Advice for updating One Identity Manager](#) on page 69.

To update an existing One Identity Manager installation to version 8.1

1. Run all the consistency checks in the Designer in **Database** section.
 - a. Start the Consistency Editor in the Designer using 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. Start the check by selecting the **Consistency check | Run** menu item.

All the database tests must be successful. Correct any errors. Some consistency checks offer repair options for correcting errors.

2. Update the administrative workstation, on which the One Identity Manager database schema update is started.

- a. Execute 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.

NOTE: To update a One Identity Manager History Database installation, change to the **Other Products** page and select the **One Identity Manager History Database**.

- c. Click **Install**.

This starts the installation wizard.

- d. Follow the installation instructions.

IMPORTANT: Select the directory you used for your previous installation as the installation directory on the **Installation settings** page. Otherwise the components are not updated and a new installation is created in the second directory instead.

3. (From version 7.0.x or version 7.1.x) End the One Identity Manager Service on the server that processes direct database queries.

(From version 8.0.x) End 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 to **130** and change the value if required.
6. Run the One Identity Manager database schema update.
 - Start the Configuration Wizard on the administrative workstation and follow the instructions.

7. (From version 7.0.x or version 7.1.x) Update the One Identity Manager Service on the server that processes direct database queries.

(From version 8.0.x) Update the One Identity Manager Service on the update server.

- a. Execute 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.

NOTE: To update a One Identity Manager History Database installation, change to the **Other Products** page and select the **One Identity Manager History Database**.

- c. Click **Install**.

This starts the installation wizard.

d. Follow the installation instructions.

IMPORTANT: Select the directory you used for your previous installation as the installation directory on the **Installation settings** page. Otherwise the components are not updated and a new installation is created in the second directory instead.

8. Check the One Identity Manager Service's login data. Revert to the original settings if the One Identity Manager Service did not initially use the local system account for logging in. Enter 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 8.1

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 execute the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

- Check whether the process `DPR_Migrate_She11` 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 73.

To update an application server to version 8.1

- 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 Portal to version 8.1

NOTE: Ensure that the application server is updated before you install the Web Portal. As from version 7.1. and later, the Web Portal requires an application server with a search service installed on it.

- To update the 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 Portal, uninstall the existing Web Portal and install the Web Portal again. For more information, see the *One Identity Manager Installation Guide*.

To update the Operations Support Web Portal to version 8.1

1. Uninstall the Operations Support Web Portal.
2. Install an API Server and compile the HTML application **Operations Support Portal**. For more information, see the *One Identity Manager Installation Guide*.

To update the Manager web application to version 8.1

1. Uninstall the Manager web application
2. Reinstall the Manager web application.
3. The default Internet Information Services user requires edit permissions for the Manager's installation directory to automatically update the Manager web application. Check whether the required permissions exist.

Applying patches to synchronization projects

⚠ CAUTION: Patches do not change customizations in synchronization projects. This means that conflicts may occur if patches are applied to synchronization projects, which have been customized. This 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. Deactivate the synchronization project.

ℹ 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. Open the synchronization project in the Synchronization Editor.
2. Select **Edit | Update synchronization project...** from the menu.
3. In **Available patches**, select the milestone you want to implement.
In **Details - Installation summary**, all dependent patches are displayed in order of installation.
4. Click **Apply selected patches**.
5. Enter any user input as prompted.
6. (Optional) In **Available patches**, select the patches for new functions that you want to apply. Multi-select is possible.
In **Details - Installation summary**, all patches are displayed in order of installation.
7. Click **Apply selected patches**.
8. Enter any user input as prompted.
9. Use the patch log to check whether customization need to be reworked.
10. If required, rework customizations in the synchronization configuration.
11. Run a consistency check.
12. Simulate the synchronization.
13. Activate the synchronization project.
14. 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 more detailed information about updating synchronization projects, see the *One Identity Manager Target System Synchronization Reference Guide*.

See also:

- [Modified synchronization templates](#) on page 52
- [Patches for synchronization projects](#) on page 54

Verifying successful installation

To determine if this version is installed

- Start the Designer or the Manager and select the menu item **Help | Info**.
You can see an overview of your system configuration on the **System information**.

The version number 2019.0001.0021.0000 for all modules and the application version 8.1 2019-01-21-031 indicate that this service pack is installed.

Additional resources

Additional information is available from the following:

- [One Identity Manager support](#)
- [One Identity Manager online documentation](#)
- [Identity and Access Management community](#)
- [One Identity Manager training portal](#)

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 or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

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

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

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

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.




Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**
-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.**