One Identity Manager 8.0

Release Notes

December 2017

These release notes provide information about the One Identity Manager release. For changes to the Web Designer and the Web Portal since the last version, see the document "Web Designer and Web Portal Changes".

The 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

About One Identity Manager 8.0

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

Every 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 Manager 8.0 is a major release with enhanced features and functionality. See Features on page 2 and Enhancements on page 9.

Features

New features in One Identity Manager 8.0:

Basic functionality

- SQL Server 2017 is supported.
- Oracle Database 12.2 is supported.
- Improved security measures for accessing the One Identity Manager.
  - Cyclical checking of authentication for existing connections.

    The system runs validity checks for open connections to prevent users from working with existing connections if they have been deactivated after they logged in. The check is carried out by the next permissions-based action on the connection after a configurable interval of 20 minutes. The interval is defined in the configuration parameter "Common\Authentication\CheckInterval".
  - Support for password policies in the One Identity Manager.

    You can implement password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

    A default password policy is supplied that protects the password for system users and employee-based authentication modules. Other predefined password policies are also supplied.
  - Support for expired passwords.

    The user is advised that their password is about to expire and can change the password if necessary. In the case of employee-based authentication modules, the system sends reminder emails starting from 7 days before the password's expiry date. You can configure the time in days in the configuration parameter "Common\Authentication\DialogUserPasswordReminder". The emails are triggered by a schedule and use the mail template "Employee - system user password expires".

    To prevent password of certain system users from expiring, you can mark these system users so that their passwords never expire.

    - Issues a random, temporary passcode for a one-off login on the Password Reset Portal.
    - Support for password history.
    - Failed login attempts are logged.
    - Wrong answers to the password question for resetting the central password are logged.
    - Login with empty passwords is no longer supported.
    - Restricted password lists are supported.
- Support for load balancing of all SQL processes.

  A new server function "SQL processing server" is available. The server can execute SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
- Improved identification of the server for automatic software updating.

  A new server function "Update server" is available. This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that the One Identity Manager database is installed on.

  The server installed with the One Identity Manager database, is labeled with this functionality during initial installation of the schema.
- Preparing data for faster cross-table searching.

  The values for columns can be prepared for faster cross-table searching. Searching for single values in MVP columns is supported.

  The functionality can be used for finding a unique central user account, for example, or a unique default email address for an employee. Columns in the default installation, which are taken into account when mapping the central user account or an email address, are labeled accordingly.
- Fallback for translations can be disabled for columns that are labeled as translation targets. Another value "Without fallback translation source" has been added to do this.
- The priority of process steps can be determined dynamically at time the process is generated.
- Support for more than one script with the same name and identical number of parameters but different data types. The data type of the script parameter can be passed in the process parameter "ScriptName" in addition to the script name, in the process component "ScriptComponent".
- The Report Editor uses an updated version of the report engine, which provides new functions and controls for setting up reports.
- A role-based authentication module for LDAP is available.
- The configuration of initial data for LDAP authentication modules is done with the configuration parameters "TargetSystem\LDAP\Authentication", "TargetSystem\LDAP\Authentication\Authentication",

"TargetSystem\LDAP\Authentication\Port",
"TargetSystem\LDAP\Authentication\RootDN" and
"TargetSystem\LDAP\Authentication\Server".

The initial configuration data for existing installations remains valid and is used as a fallback.

Web Portal

- New Password Reset Portal.

  The Password Reset Portal allows users to reset passwords of the user accounts they manage, securely. Users can navigate from the Web Portal directly to the Password Reset Portal.

  To utilize the Password Reset Portal, it must be installed as a dedicated web application. The required security is guaranteed by Starling Two-Factor Authentication.

- New Operations Support Web Portal.

  The Operations Support Web Portal supports help desk users with their tasks in One Identity Manager. You can use the Operations Support Web Portal to create passcodes, display DBQueue and Job queue entries for specific objects, show process steps and restart them if necessary, monitor processing handling performance.

  To utilize the Operations Support Web Portal, it must be installed as a dedicated web application. A new application role **Base roles | Operations support** is provided for use with the Operations Support Web Portal. The required security is guaranteed by Starling Two-Factor Authentication.

- To improve user friendliness, the Web Portal's user interface and the navigation structure has been completely reworked and new functions have been added.
  - Support for the Starling 2FA App for multi-factor authentication.

    In addition to the login, a further access control (multi-factor authentication) can be configured.
  - Managers can generate a passcode for their staff.
  - Users can set their password question and answer.
  - New wizards for defining reports and report subscriptions.
  - Bookmarks for service categories can be added.
  - Changed data values are marked.
  - Processes triggered by users are displayed.
  - Users specify whether diagrams are permanently hidden.
  - Managers can view their staff's rule violations.
  - The chief approval team can immediately escalate a request.
  - Owners of departments, location and cost centers can also manage child objects.
  - Request templates can be created from a reference user and its assignments.

- Request templates can be created for assignment requests.
- Permissions, which contribute to a rule violation can be removed.
- An additional test of possible exclusion definitions is made before sending a request.
- A product can be unsubscribed for several people at the same time, also for multi-requestable/unsubscribable resources.
- Renewals and cancellations do not have to be done strictly through the shopping cart.
- Users can temporarily switch to another language.

Web Designer

- New version of the Secure Token Server. For more information, see the document "Web Designer and Web Portal Changes".
- Custom configuration settings for a given web project can be managed in a central overview.

Target system connection

- Support for G Suite as a target system. The key aspects are the mapping of user accounts and their entitlements. To do this, groups, organizations, permissions, admin roles, products and SKUs are mapped in One Identity Manager.
- Support for Oracle E-Business Suite as a target system. The key aspects are the mapping of user accounts, responsibilities and entitlements.
- Support for SharePoint Online as target system. The key aspects are the mapping of user accounts, groups, site collections, sites, roles and role assignments. The SharePoint Online connector and a default project template are installed.
- Mapping remote mailboxes for Exchange hybrid support. The mapping for remote mailboxes is part of the Microsoft Exchange project template. Remote mailboxes are synchronized using the Microsoft Exchange connector.
- The member filter's excluded lists for the target system Microsoft Exchange have been altered in connection with Exchange hybrid support.

  A patch for synchronization projects with the patch ID VPR#28904 is available.
- Support for Outlook Web App mailbox policies for the Microsoft Exchange target system.
- The way the Microsoft Exchange version is determined has been changed. The schema property `ObjectVersion` is used to determine the version.

  A patch for synchronization projects with the patch ID VPR#27447 is available.
- The Microsoft Exchange connector now supports connections through HTTPS.

  NOTE: Microsoft Exchange does not support this type of connection by default. You must configure support for HTTPS in your Microsoft Exchange.

- The schema property "Recovery" is provided to mark Microsoft Exchange mailbox databases as recovery databases.
- Introduction of a revision filter for Microsoft Exchange.

  Microsoft Exchange synchronization has been changed as follows to support customer environments with large numbers of objects:

  1. The schema type "Mailbox" has been divided into the sub types "Mailbox", "Calendar Processing" and "Mailboxstatistics".
  2. A revision criterion has been defined for the schema types "Mailbox", "MailUser", "MailContact", "MailPublicFolder", "DistributionGroup" and "DynamicDistributionGroup". This is based on the "whenChanged" property of the underlying Active Directory object.
  3. Automatic dependency resolution of the synchronization workflow's steps has been disabled, which has reduced the number of synchronization steps.

     Due to this, reference objects arise in the synchronization buffer during synchronization (`DPRAttachedDataStore`), possibly at short notice, which are resolved afterward by a maintenance step. This happens exclusively on the One Identity Manager side, therefore requiring no other access to the Microsoft Exchange infrastructure.

  IMPORTANT: The revision algorithm can only be enabled in synchronization projects created with version 8.0. If usage of revisions is activated in old 7.x synchronization projects, modifications made directly in Microsoft Exchange are not necessarily recognized.

  NOTE: Due to the complexity of the changes, existing synchronization projects are not automatically converted by using the patch. You can, however, continue to use existing synchronization projects (from 7.x installations), unchanged until the next major release because the schema is compatible. The properties of the old "mailbox" schema type that has been transferred to the new schema types named above, are marked as obsolete in the "mailbox" type. This does not, however, have any affect on the functionality. These properties will certainly be removed in the next major release.

  Even if your 7.x synchronization projects are compatible, it is recommended you recreate the synchronization project using the synchronization project template implemented in the version 8.0.
- Introduction of a revision filter for Exchange Online.

  Exchange Online synchronization has been changed as follows to support customer environments with large numbers of objects:

  1. The schema type "Mailbox" has been divided into the following types:
     - Mailbox (Basic information about mailboxes)
     - CalendarProcessingSettings_RoomEquipment (calender processing settings for room and equipment mailboxes)

- CalendarProcessingSettings_UserShared (calender processing settings for user and room mailboxes)
- MailboxStatistics_RoomEquipment (status information for room and equipment mailboxes)
- MailboxStatistics_UserShared (status information for user and room mailboxes)

2. A revision criterion has been defined for the schema types "Mailbox", "MailUser", "MailContact", "MailPublicFolder", "DistributionGroup", "UnifiedGroup" and "DynamicDistributionGroup". This is based on the "whenChanged" property of the underlying Azure Active Directory object.
3. Automatic dependency resolution of the synchronization workflow's steps has been disabled, which has reduced the number of synchronization steps. Due to this, reference objects arise in the synchronization buffer during synchronization (`DPRAttachedDataStore`), possibly at short notice, which are resolved afterward by a maintenance step. This happens exclusively on the One Identity Manager side, therefore requiring no other access to the Exchange Online infrastructure.
4. The synchronization steps for `CalendarProcessingSettings_UserShared` and `MailboxStatistics_RoomEquipment` are disabled by default. Calendar processing settings for user mailboxes (`CalendarProcessingSettings_UserShared`) are not usually relevant but can be queried by the appropriate commands. The same is valid for status information (for example, the number of emails, last login) from room and equipment mailboxes (`MailboxStatistics_RoomEquipment`). The steps in the workflow "Initial Synchronization" can be enabled at any time if required. However, this can cause a noticeable increase in the runtime.

IMPORTANT: The revision algorithm can only be enabled in synchronization projects created with version 8.0. If usage of revisions is activated in old 7.x synchronization projects, modifications made directly in Exchange Online are not necessarily recognized.

NOTE: Due to the complexity of the changes, existing synchronization projects are not automatically converted by using the patch. You can, however, continue to use existing synchronization projects (from 7.1.2 installations), unchanged until the next major release because the schema is compatible. The properties of the old "mailbox" schema type that has been transferred to the new schema types named above, are marked as obsolete in the "mailbox" type. This does not, however, have any affect on the functionality. These properties will certainly be removed in the next major release.

Even if your 7.1.2 synchronization projects are compatible, it is recommended you recreate the synchronization project using the synchronization project template implemented in the version 8.0.

- The LDAP connector supports connections at rootDSE level.
- The LDAP connector provides information about object class hierarchy.
- The Windows PowerShell connector supports `SecureString` parameters.

A `ConversionMethod` can now be entered in the `SetParameter` definition. The `ConversionMethod="ToSecureString"` is currently supported. This allows connections parameters to be passed securely.

- Extensions in the Synchronization Editor
  - New view for managing custom project templates in expert mode.
  - Synchronization workflows can be copied.
  - A schema editor for improved editing of virtual properties is integrated in the Schema Browser.
  - Start up configurations can be grouped. Behavior for simultaneous start up within a group can be defined.

    The delay between retries is specified in the configuration parameter "Common\Jobservice\RedoDelayMinutes".
  - Comprehensive logging and improved displaying of entries in the system journal.
  - New virtual property of type "Data mapping" for mapping predefined value lists.
  - New schema class type "Unique Objects" for creating unique objects to simplify the import of multiple object types from a single source such as a CSV file or a database table.
  - Patches can be automatically applied during One Identity Manager schema updates.

Identity and Access Governance

- Introduction and versioning of approval workflows for IT Shop requests and attestations.
  - The configuration parameters "QER\ITShop\OnWorkflowAssign" and "QER\ITShop\OnWorkflowUpdate" specify whether pending requests are reset when the approval workflow is changed.
  - The configuration parameters "QER\Attestation\OnWorkflowAssign" and "QER\Attestation\OnWorkflowUpdate" specify whether pending attestations are reset when the approval workflow is changed.

  NOTE: If you have set up you own approval procedures and have used properties from approval steps in your queries for finding approvers, modify these queries as follows:

  If you referenced the table `PWODecisionStep` over the column `UID_PWODecisionStep` until now, then change this reference to the column `UID_QERWorkingStep` in the table `QERWorkingStep`.
- The approval step of an attestation case can be used to specify whether the employee affected by the attestation case can also approve it. This overrides the setting in the configuration parameter "QER\Attestation\PersonToAttestNoDecide".

- Assignment resources can be created for One Identity Manager application roles. The assignment resource can be requested in the Web Portal like any other company resource. After the request has been successfully assigned, the employee, for whom it was requested, becomes a member of the associated application role through internal inheritance processes.

See also:

- Enhancements on page 9
- Fixes on page 19
- Schema changes on page 27
- Patches for synchronization projects on page 34

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.0.

Table 1: General known issues

Enhancement	Issue ID
An employee's main identity can now be used for authentication with the authentication module "Person".	27863, 3962834
Improved performance in the DBQueue Processor.	27284, 28522, 28569, 27675, 4064153, 4064153
Labeling of DBQueue Processor tasks for load limiting. Limits for changes within an operation are configured in the configuration parameters "QBM\DBQueue\ChangeLimitMin" and "QBM\DBQueue\ChangeLimitMax".	12081
Dynamically determining statistics under Oracle Database. This is configured in the configuration parameter "QBM\DBQueue\OptimizerDynamicSampling".	28004
Tasks that require a connection to the application server are displayed in the Launchpad.	26864
Instead of only offering access to single values, an entity (and therefore all its values), accessed by FKs can now be returned through the `IEntityWalker`.	27105
Improved configuration options for importing transport with change labels.	26557
Improved monitoring of the entire Job queue in Job Queue Info.	26785

Enhancement	Issue ID
Improved identification of database staging levels by modifying colors in the status bar in all front-ends.	27148
Columns with a list of permitted values can be added in the full text search.	27469, 667442
Pending changes are now displayed in the Manager.	26340
Favorites can be removed in the Manager using the context menu.	27043
Improved display of permissions group hierarchy in the User & Permissions Group Editor.	26956, 28195, 4054136
The Language Editor now displays the language available in the front-end as optional languages for translation.	28359
Clarified error message `[810025] User accounts: Write permission denied.`	28587, 4087337
Improved update behavior for the One Identity Manager Service automatic software update.	28650
Improved error logging in the process component "FileComponent".	28656, 4093596
Minimum process query interval set to 10 seconds for the Job service.	27112, 3867374
Multiple One Identity Manager Service instances can be installed on one server using One Identity Manager Installation Wizards and the Server Installer. The different installation directories are numbered sequentially.	27231, 3965347
Out-Parameters are shown in the process history.	27237
The SQL Editor in the Designer and the Object Browser support auto-completion.	27688
The Script Editor in the Designer supports auto-completion for configuration parameters.	27422
Improved sorting by column in the Schema Editor in the Designer.	27482
Improved representation of result lists in the SQL Editor in the Designer and the Object Browser.	27445
Improved display of base data in the Designer.	28246
Customizations to default processes and default tables displayed in the Designer.	28230
Hidden parameters are displayed by a new program function in the Job Queue	27665,

Enhancement	Issue ID
Info. To use this function, assign the respective permissions groups to the program function "JobQueue_ShowHiddenParameters"	3975588
The columns that trigger templates can be displayed in the Designer.	27852
Improved generation of indexes.	27921, 3988910
Extended functions for editing change labels in the Manager and the Designer. The changes sort order can be modified. You can search inside the change labels. The change label's XML data can be edited.	26894
Improved transporting by change label.	28011
Syntax check for preprocessor condition now takes place on saving.	28021, 4053085, 4053085
Improved the Software Loader to prevent error conditions.	28158, 4051728
Custom event can now be added to default processes in the Designer.	28231
IT Shop tags can be transported.	28418, 4085515, 4085518
The generic form "VI_Generic_MasterData" supports the definition of bit masks.	28536
Improved representation of schema tables extensions in the Web Designer.	26980, 3705851
Improved definition of indexes in the Schema Extension program.	28598, 4064153
Optimized the Database Transporter to prevent deadlocks when transporting schema extensions.	28603, 4107215
Data modifications are no longer possible in the One Identity Manager database when triggers are disabled.	28610, 4107215
Improved re-enabling of triggers and constraints.	28637, 4107215, 4109588
The System Debugger differentiates between system scripts and custom scripts when exporting.	27667
The System Debugger can be used to upload templates, formatting scripts, table scripts and method definitions.	27918

Enhancement	Issue ID
Language culture codes can now be used in #LD notation in scripts.	28852
The configuration parameter "Common\ProcessState\ProgressView\WaitInJobChain" has been deleted. Customized usage might required modification.	27870

Table 2: General Web Portal and Web Designer

Enhancement	Issue ID
The authentication module setting installed in the Web Portal and the Web Designer is limited to authentication modules that are not capable of SSO.	20870, 690405
Certain CSS outlines are only shown in accessibility mode for visual reasons.	655773
The component VI_Edit_MultiValueProperty for entering multi-value properties has been reworked.	26254, 657785
The views 'Object state' and 'Solution' have been merged.	24475, 673888
The special definition of Hyper Views has been removed from the Web Portal code. The view is now exclusively generated from the content of the table `DialogTree`.	674809, 692057
The Master/Detail control supports low resolution better.	673729
Visual representation of read-only properties has been reworked.	676883
Visual representation of the heatmap has been reworked.	677380, 677385
Edit functions in the component `VI_Roles_RolesAndEntitlements` have been moved to the ObjectSheet component.	25974, 677572
A switch for controlling object dependent references has been added.	25841, 677573
Some unused images have been removed from the `WebDesigner.ImageLibrary.dll`.	677574
Code branches for desktop and mobile views have been standardized in the form templates.	678334
The old data model for configuring search fields has been removed because the search index can be used instead.	27088, 678805
The Web Portal login page has been adapted for low resolution.	678828
Some Web Portal functions cannot be used sensibly on smartphones. In these cases, an appropriate message is displayed.	715853

Enhancement	Issue ID
Option for automatically deriving a grid's lists view from the grid definition.	692572
The new composition API is available for use over .NET.	681359
A list view, which is optimized for smartphones can be defined for a grid in addition to a table-based view.	691223
There is an option for always displaying a grid as a list view.	692352
Processing of an employee's data is centralized in the component `VI_Common_ObjectSheet_Person`.	693277
Some properties, node types and values are marked as "obsolete".	693528
Optional condition for the grid, whether row selection is enabled for a specific row.	693632
Validator conditions can be defined in the control tree.	694767
Captcha is automatically updated after incorrect input.	27671, 694770
The compiler checks object dependent links for ambiguity and generates an error message.	694783
The compiler checks whether an element's identifier starts with the correct module prefix.	695006
Option for hiding a grid column in the automatically generated list view.	695200
"Create interactive entities" is disabled for new objects.	25800, 695769
The timeout for a Web Designer module's inactivity can be configured globally.	697175
New function "Try to fix compiler messages".	698451
Forwarding within forms of a form component is now possible.	705753
Improved handling of user configuration (`QBMXUser`), if a non-employee related authentication module is used.	706324
In the Master/Detail control the threshold for switching between vertical and horizontal view has been optimized.	706509
There is now a property on an extension to disable it.	710612
Custom controls can be added in the grid control header.	711465
Improved handling of control for auto-completion.	711679
Which button is linked to the ENTER key can be controlled in the component for displaying popups.	714531
The total number or results is shown in grids.	715617

Table 3: Target system connection

Enhancement	Issue ID
Faster loading of synchronization projects in the Synchronization Editor.	27555
Diverse optimizations of the synchronization buffer and cache behavior.	26832, 27662, 27563, 28350, 28576
Improved behavior of the Synchronization Editor when working with encrypted values. The default value of the configuration parameter "DPR\UI\EncryptedValueHandling" has been changed to "IgnoreAll". This means the encryption dialog is not shown when the synchronization project is opened. All encrypted values are ignored by default.	27274
German display names of property mapping rules and virtual schema properties are converted to English. A patch for synchronization projects with the patch ID VPR#28560 is available.	28560
Converts connection parameter names and values. A patch for synchronization projects with the patch ID VPR#27769 is available.	27769
Optimized pre-scripts for generating target system relevant processes.	28042, 3859791
The domain object SID is determined by Active Directory synchronization. A patch for synchronization projects with the patch ID VPR#27457 is available.	27457
When Active Directory group memberships are synchronized, the global catalog query for resolving the SID is not carried out. The mapping "group" has been extended with additional virtual schema properties. A patch for synchronization projects with the patch ID VPR#27997 is available. NOTE: When the mode for member publishing (task "Configure tables for publishing") in Active Directory is changed from "Enable merging" (default) to do not "Enable merging", the mapping rules, which allows members to be written to the Active Directory group, must be changed.	27997
Improved mapping SAP license information for system measurement. A patch for synchronization projects with the patch ID VPR#27289 is available.	27289
Improved transfer of the validity period for SAP role assignments and memberships in structural profiles.	26883, 28031, 3677202, 4041294, 4054671

Enhancement	Issue ID
The schema type SAPRCRange has been removed. A patch for synchronization projects with the patch ID VPR#27539 is available.	27539
An additional tab for passwords is displayed on the Unix user account's master data form.	27947
Optimized provisioning of objects changes for the Universal Cloud Interface interface. A patch for synchronization projects with the patch ID VPR#27371 is available.	27371
Changed the SCIM interface's property mapping rules for the schema properties "id", "canonical name" and "distinguished name" to the new schema properties added for them in the One Identity Manager schema. A patch for synchronization projects with the patch ID VPR#27860 is available.	27860
Email notifications can be configured through login data in the case of custom target systems. This is configured in the configuration parameter "TargetSystem\UNS\Accounts\InitialRandomPassword" and its sub-parameters.	28111
The following configuration parameters have been deleted. When you update One Identity Manager version 7.x to version 8.0, the configuration parameter settings for forming passwords are passed on to the target system specific password policies. Configuration parameters for Azure Active Directory • TargetSystem\AzureAD\Accounts\InitialPassword • TargetSystem\AzureAD\Accounts\InitialRandomPassword\Character • TargetSystem\AzureAD\Accounts\InitialRandomPassword\Length • TargetSystem\AzureAD\Accounts\InitialRandomPassword\Numeric • TargetSystem\AzureAD\Accounts\InitialRandomPassword\SpecialCharacter • TargetSystem\AzureAD\Accounts\InitialRandomPassword\UpperCase Configuration parameters for Active Directory • TargetSystem\ADS\Accounts\InitialPassword • TargetSystem\NDO\Accounts\InitialRandomPassword\Character • TargetSystem\ADS\Accounts\InitialRandomPassword\Length • TargetSystem\ADS\Accounts\InitialRandomPassword\Numeric • TargetSystem\ADS\Accounts\InitialRandomPassword\SpecialCharacter	28111

Enhancement	Issue ID
• TargetSystem\ADS\Accounts\InitialRandomPassword\UpperCase Configuration parameters for the new Universal Cloud Interface interface • TargetSystem\CSM\Accounts\InitialPassword • TargetSystem\CSM\Accounts\InitialRandomPassword\Character • TargetSystem\CSM\Accounts\InitialRandomPassword\Length • TargetSystem\CSM\Accounts\InitialRandomPassword\Numeric • TargetSystem\CSM\Accounts\InitialRandomPassword\ SpecialCharacter • TargetSystem\CSM\Accounts\InitialRandomPassword\UpperCase Configuration parameters for LDAP • TargetSystem\LDAP\Accounts\InitialPassword • TargetSystem\LDAP\Accounts\InitialRandomPassword\Character • TargetSystem\LDAP\Accounts\InitialRandomPassword\Length • TargetSystem\LDAP\Accounts\InitialRandomPassword\Numeric • TargetSystem\LDAP\Accounts\InitialRandomPassword\ SpecialCharacter • TargetSystem\LDAP\Accounts\InitialRandomPassword\UpperCase Configuration parameters for IBM Notes • TargetSystem\NDO\Accounts\InitialPassword • TargetSystem\NDO\Accounts\InitialRandomPassword\Character • TargetSystem\NDO\Accounts\InitialRandomPassword\Length • TargetSystem\NDO\Accounts\InitialRandomPassword\Numeric • TargetSystem\NDO\Accounts\InitialRandomPassword\ SpecialCharacter • TargetSystem\NDO\Accounts\InitialRandomPassword\UpperCase Configuration parameters for SAP R/3 • TargetSystem\SAPR3\Accounts\InitialPassword • TargetSystem\SAPR3\Accounts\InitialRandomPassword\Character • TargetSystem\SAPR3\Accounts\InitialRandomPassword\Length • TargetSystem\SAPR3\Accounts\InitialRandomPassword\Numeric • TargetSystem\SAPR3\Accounts\InitialRandomPassword\ SpecialCharacter	

Enhancement	Issue ID
• TargetSystem\SAPR3\Accounts\InitialRandomPassword\UpperCase Configuration parameters for Unix • TargetSystem\Unix\Accounts\InitialPassword • TargetSystem\Unix\Accounts\InitialRandomPassword\Character • TargetSystem\Unix\Accounts\InitialRandomPassword\Length • TargetSystem\Unix\Accounts\InitialRandomPassword\Numeric • TargetSystem\Unix\Accounts\InitialRandomPassword\SpecialCharacter • TargetSystem\Unix\Accounts\InitialRandomPassword\UpperCase	
The following configuration parameters have been deleted. Customized usage might required modification. Configuration parameters for Active Directory • TargetSystem\ADS\IsOperational • TargetSystem\ADS\RedoDelay Configuration parameters for IBM Notes • TargetSystem\NDO\IsOperational • TargetSystem\NDO\RedoDelay Configuration parameters for SAP R/3 • TargetSystem\SAPR3\IsOperational • TargetSystem\SAPR3\RedoDelay • TargetSystem\SAPR3\SingleThread Configuration parameters for SharePoint • TargetSystem\SharePoint\IsOperational • TargetSystem\SharePoint\RedoDelay • TargetSystem\SharePoint\SingleThread	28607

Table 4: Identity and Access Governance

Enhancement	Issue ID
The employee's overview reports have been extended to include additional information about assigned entitlements and sub identities.	26847
Report that provide the number of employees that are assigned to a	27913

Enhancement	Issue ID
department, a cost center or a location, have been extended by a grouping by identity types.	
Permitted values for employees' identity types have been extended by the value "Machine identity".	28324
The company can be set for internal and external employees.	28573
Employees can be deleted from the One Identity Manager using the procedures `QBM_PDeleteDeep`.	27643, 2657573
Improved tooltips in a request's approval sequence.	28540
The approval history shows whether the approval decision was met based on a delegation.	27431
Improved performance loading attestation cases.	28582, 4100881
Inactive employees are excluded when determining approvers and attestators.	27815, 4011577
The configuration parameter "QER\ITShop\ResetOnWorkflowChange" has been deleted. The old configuration parameter setting is not converted to the new configuration parameter.	13224
The configuration parameter "QER\Person\CentralPasswordHistoryLength" has been deleted. The value of the configuration parameter is copied to the password policy for the employees central password.	28666

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 34

Deprecated features

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

- Provider mode, including the associated process component "ObjectTransferComponent".

  The One Identity Manager connector can be used for transporting data between One Identity Manager databases. For more detailed information about synchronizing using the One Identity Manager connector, see the One Identity Manager User Guide for the One Identity Manager Connector.

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

- Oracle Database as database system for the One Identity Manager database (no longer available after release of One Identity Manager version 8.1)

Fixes

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

Table 5: General known issues

Fix	Issue ID
Error in the History Database if the Oracle procedure `PProcessGroupDelete` is called whilst running the process `VI_SourceDatabase_Import`.	28725, 4113915
New files are not distributed by automatic software update if they were imported by transport into the One Identity Manager database.	27625, 3900149, 4024883
Custom scripts in the script library are automatically overwritten by the automatic software update.	27667, 3896466
The task `QBM-K-JobqueueOverviewInvalid` is queued to frequently in the DBQueue.	28367, 4064153
It is possible to create new entries in `QBMGuidReplace` although `GUIDReplace` is already running.	28432, 4090349
The program Schema Extension is terminated immediately and without prompting, after pressing **ESC**.	28480, 4087262
The write access of a custom permissions group for a custom column disappears if the permissions group has read access to at least one other regular column.	28481, 4068237
Data Import only reads the first line in a CSV file if the line break only consists of "CR".	28483, 4088573
Different errors adding and editing custom configuration parameters.	28492, 28493, 4071473
Consistency check fails if a foreign key column of a view is added in a simple table.	28497, 4045308, 4080035
Error in the Database Transporter if custom columns of default tables are imported, which do not have the prefix "CCC_".	28524
Error in Manager if changes are logged for the table `DialogTag`.	28544, 4075754

Fix	Issue ID
Error in the script `VID_GetRunningOSfromServer`.	28565, 4084084
The configuration supplied in the global configuration file (`globallog.config`) occasionally causes messages to be thrown out of the error log file if there is a high rate of log entries.	28568, 4075429
A previously configured HTTP authentication is not displayed if the program Job Service Configuration is restarted.	28571, 4081445
If a custom translation is deleted in the Manager, the associated entry in the table `DialogMultiLanguage` is not deleted.	28613, 4100028
If primary keys changed by migration, it might result in invalid references.	28614, 4079826
Objects exports as a ZIP file from Manager might be different to the same export from the Database Transporter.	28629, 4062338
The configuration parameter "Common\AutoExtendPermissions" also affects custom permissions groups.	28709, 4115806
Single step mode does not work when debugging a database project in the Web Designer.	28347, 3914817
An error message is shown in the transport package description of a package being loaded by the Database Transporter that was created in Manager.	28629, 4062338
Validation script does not work properly when accessing parameter sets in the Report Editor.	28806, 4110991
Passwords of default system users are marked as "expired". This makes it impossible to carry out an installation or to log in with the default system user. Custom system users are not affected. All new installations and updates of version 8.0 after the 9th December 2017 are affected. This fix deals with the problem described in the knowledge article under https://support.oneidentity.com/kb/235185.	29170, 4170482-1

Table 6: Target system connection

Fix	Issue ID
Error adding computer objects in Active Directory.	28293, 4068230
A system filter in the scope definition is not taken into account when synchronizing an Active Directory domain.	28501, 4093584

Fix	Issue ID
If the task **Unlock user account** is run on an Active Directory user account, the user account remains locked.	28638, 4090604
Error executing the process `ADS_ADSDomain_Maintain ADSOtherSID_PostSync` for an Active Directory domain managed by Active Roles.	27571, 4075290
Active Roles specific properties of Active Directory objects cannot be edited if there is also an Active Directory synchronization project for the domain.	28589, 4074695
Error in the formatting script for the column `LDPDomain.Ident_Domain`.	28619, 4099296
Error in the SAP R/3 connector during SNC authentication.	24742, 3253751
If an SAP user account's membership in a single role is deleted in One Identity Manager, the change is not provisioned.	28048, 4096475
An error occurs if all the telephone numbers of an SAP user account are deleted at the same time.	28529, 4073192
If a schema type has several columns marked with `IsUniqueKey`, only the first one is used to create the prototype object during provisioning.	27584, 4096785
Diverse error on the form "Define search criteria for employee assignment".	28547, 4095553
Identification and correction of invalid changes does not work for many-to-many schema types in property mapping rules.	27476, 4102364
Error adding a new mapping with the mapping wizard, which based on an existing mapping.	28538, 4101927
Error using "$$" in a database user's password if the One Identity Manager database is encrypted.	28556, 4101908
If two synchronizations with the same start up configuration are started at the same time, a synchronization, which is already running, is not always correctly identified.	28673, 4079945
After successful provisioning of memberships, the "outstanding" label must be reset. A patch for synchronization projects with the patch ID VPR#27304 is available.	27304

Table 7: Identity and Access Governance

Fix	Issue ID
If the method `CreateITShopOrder` is called to transform a membership in hierarchical roles into an assignment request, the Customizer gets stuck in an	28037, 3997275

Fix	Issue ID
infinite loop if the base object is loaded as deferred object.	
The subject in the mail template "Attestation - Approval by mail" uses an invalid column.	28251

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 34

Known issues

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

Table 8: 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 Database Compiler ends without compiling the database, the task remains in the DBQueue.	3209411, 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 SQL query and use aliases for the affected columns.	23521
Error message in the Web Designer query window: "Access to the path ... is denied." This error occurs if the user the web application process runs under, does not have write permissions for the given folder.	23769
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
"Read Only" type tables with Common Table Expressions (CTE) in the ViewAddOn are not added in the schema. In One Identity Manager 7.0, behavior has been modified if you use common table expressions with the keyword `with` as a condition for view definitions in	

Known Issue	Issue ID
read-only tables. The conditions for view definitions are embedded in a summary query. This means, you cannot be sure that a common table expression is the very first expression in a query. Possible error message: `(execute slot single)50000 0 re-throw in Procedure QBM_ZViewBuildR, Line 1050000 0 re-throw in Procedure QBM_PViewBuildR_intern, Line 10250000 0 re-throw in Procedure QBM_PViewBuildR_intern, Line 8250000 0 re-throw in Procedure QBM_PViewBuild_FromAddOn, Line 6550000 0 re-throw in Procedure QBM_PSQLCreate, Line 26156 0 detected in (...) Procedure ..., Line 6156 0 Incorrect syntax near the keyword 'with'` Recommended action: Check custom view definitions. 1. Create a view under common table expression usage. Example: `create view CCC_Vxy as` `with a (col1, col2) as (` `select 1 as col1, 2 as col2` `)` `select * from a` `go` 2. Use the view in the additional view definition (`QBMViewAddon`) of the read-only table. `select * from CCC_Vxy`	
Number of parameter pairs "ParamName"/"ParamValue" in the MailComponent's process task "SendRichMail" is not always sufficient. 10 parameter pairs are available by default. If this number is not sufficient, you can add additional custom process parameters, which Process Editor can then use as parameters. This function is available as from One Identity Manager version 7.0.	25164
In certain circumstances, objects can be in an inconsistent state after simulation in the 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. This problem only occurs	3372460, 25315

Known Issue	Issue ID
if the Configuration Wizard is started directly. Always use `autorun.exe` for installing One Identity Manager components. This ensures that you do not select any invalid modules.	
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. Solution: Change the permissions for the users on parent folder of the web application (by default `C:\inetpub\wwwroot`) and apply the changes. Then revoke the changes again.	26739
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.	3775973, 27203
Error connecting through an application server if the certificate's private key, used by the VI.DB to try and encrypt its session data, cannot be exported and the private key is therefore not available to the VI.DB. Solution: Mark the private key as exportable if exporting or importing the certificate.	3981140, 27793
`DialogTable.OnLoadingScript` is no longer supported.	27968
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, 4081234
Error in the SQL Formatter if a Boolean attribute supplies a 'NULL' value. The default value is '0'.	28381, 4063027
Database error migrating a database in an SQL Server AlwaysOn availability group. The following error occurs during a One Identity Manager schema update: `Database error 1468: The operation cannot be performed on database "<database name>" because it is involved in a database mirroring session or an availability group. Some operations are not allowed on a database that is participating in a database mirroring session or in an availability group. ALTER DATABASE statement failed.` Cause: The database is a component of an AlwaysOn availability group and the SQL Server Service Broker no longer exists. The One Identity Manager schema update tries to add the SQL Server Service Broker again. Solution: 1. Remove the database from the AlwaysOn availability group.	27919, 4039342

Known Issue	Issue ID
2. Update the One Identity Manager schema. This recreates the SQL Server Service Broker again. 3. Add the database to the AlwaysOn availability group again.	

Table 9: Target system connection

Known Issue	Issue ID
Schema properties used to identify system objects must contain a value. They cannot be empty.	23895
Automatic employee assignment for Notes user accounts does not work. Cause: `DialogObject.ObjectName` on `NDOUser` has been renamed from "NotesUser" to "NDOUser". Solution: Test the existing search criteria for employee assignment (table column `NDODomain.AccountToPersonMatchingRule`) and replace "NotesUser" with "NDOUser".	23270

An error may occur when synchronizing a target system and provisioning object modification if the synchronization project was created with One Identity Manager 7.0 and no hotfixes were installed.
Example of an error message:
`[2134002] Error executing an adhoc projection!`
`[1777239] The mapping rule (Members by SID) was unable to execute the projection between system objects (<group cn>) and (<group dn>) successfully!`
Solution: Delete the synchronization project and recreate it. Restore your customizations.
	3011731, 24022

Memory leaks occur with Windows PowerShell connections, which use `Import-PSSession` internally.	23795
After synchronizing an SAP R/3 environment, assignments of single role to SAP user accounts are labeled as pending. This problem can occur if: • SAP role assignments to user accounts were loaded before installing One Identity Manager 7.0.1. in the One Identity Manager database • Single role assignments, which are included in collective roles, were mapped as direct assignments (Error ID 3218196) By resolving this problem in One Identity Manager 7.0.1., incorrect assignments are labeled as pending after synchronizing again using the appropriate synchronization configuration.	

Known Issue	Issue ID
Solution: Delete pending assignments in One Identity Manager target system synchronization.	
By default, the building block "HR_ENTRY_DATE" of an SAP HCM system cannot be called remotely. Solution: Make it possible to access the building block "HR_ENTRY_DATE" remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate`in the Synchronization Editor.	3260098, 25401
You must provide a user account with the following permissions for full synchronization of Active Directory user accounts with the supplied One Identity Manager default configuration. • Member of the Active Directory group "Domain administrators" A sensible minimum configuration which, with respect to pure user management, differs effectively in terms of permissions from a member of the group "Domain administrators" cannot be recommended.	26350, 3612100
Very high memory usage when processing memberships in LDAP groups in an Oracle Database.	26770
Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses are stored until now.	27042
The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3. If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration. • Add a custom column to the table `SAPUser`. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required.	3777857, 27359
No passwords can be provisioned when the bind method "Fast Bind" is in use in Active Directory. The method "SetPassword" is, therefore, not available. The process step "AdhocProjection" fails with the message: `[System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKNOWNNAME))).`	27427
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.	3923873, 3932523, 27687

Known Issue	Issue ID
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.	
To use automatic employee assignment for central user administration (CUA) user accounts, assign the account definition to the CUA central system. Account definitions cannot be used to assign user accounts to child systems.	28137
Error in IBM Notes connector (`Error getting revision of schema type ((Server))`). Probable cause: The IBM Notes environment is rebuilt or numerous entries have been made in the Domino Directory. Solution: Update the Domino Directory indexes manually in the IBM Notes environment.	27126

Table 10: Third party contributions

Known Issue	Issue ID
Synchronizing a very large Active Directory system with an SQL Server database crashes with the error message (Microsoft SQL Server, error: 22022).	23524
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

Schema changes

The following provides an overview of schema changes in One Identity Manager version 7.1.2. up to version 8.0.

Configuration Module

- New column DialogColumn.SplittedLookupSupport and new table QBMSplittedLookup for preparing data for faster cross-table searches.
- New column DialogTable.DisplayNameSingular for mapping the singular form of table display names.
- New tables QBMPwdPolicy, QBMObjectHasPwdPolicy and QBMVPwdPolicyColumns for mapping password policies.
- New table QBMPwdHistory for mapping password history.
- New table QBMPwdBlacklist for defining restricted passwords.
- New columns DialogUser.BadPasswordAttempts, DialogUser.PasswordLastSet and DialogUser.PasswordNeverExpires for handling system users passwords.
- New columns Job.IsForHistory and Jobqueue.IsForHistory for specifying whether process step messages are written in the process history.
- New column Job.PriorityDefinition for defining a script, which specifies the priority depending on the contents of the process.
- New columns JobParameter.IsCompressed and JobRunParameter.IsCompressed for specifying whether the parameter's value is compressed.
- New columns QBMDBQueueTask.ExecutionDelaySeconds and QBMDBQueueTask.LastExecutedAt for mapping time of execution.
- New column QBMDBQueueTask.ChangeLimit for labeling DBQueue Processor tasks with loading limits.
- New columns QBMEventHasFeature.XMarkedForDeletion, QBMMethodHasFeature.XMarkedForDeletion and QBMScriptHasFeature.XMarkedForDeletion.
- New table QBMFileHasDeployTarget for assigning files to machine roles for automatic software updating.
- Column QBMPermissionSettingBase.Principal extended to nvarchar(23) or varchar2(23) respectively.
- Column QBMVSystemOverview.Category extended to nvarchar(20) or varchar2(20) respectively.
- Data type of column QBMVSystemOverview.Category changed to nvarchar(20) or varchar2(20) respectively.
- Column DialogDBQueue.SubObject shortened to nvarchar(38) or varchar2(38) respectively.
- Data type of columns Job.ProcessTracking and JobChain.ProcessTracking changed to bit or number(1, 0) respectively.
- The column DialogTable.OnLoadingScript has been deleted.
- The column QBMServer.UID_Database has been deleted.

Target System Synchronization Module

- New column DPRAttachedDataStore.CreationDate for mapping time of creation.
- New column DPRJournalSetup.OptionContextDisplay as display name for entries in the synchronization log.
- New column DPRNameSpaceHasDialogTable.WhereClause as condition for provisioning memberships.
- New columns DPRProjectionStartInfo.StartGroupConcurrenceBehavior and DPRProjectionStartInfo.StartGroupName for grouping start up configurations.
- New columns DPRSchemaClass.IsObsolete, DPRSchemaMethod.IsObsolete, DPRSchemaProperty.IsObsolete and DPRSchemaType.IsObsolete for marking deprecated elements.
- New column DPRShellPatch.IsAutoPatch for labeling patches that should be run automatically.

Target System Base Module

- Column TSBVDirectAssignWrong.Reason shortened to varchar(21) or varchar2(21) respectively.
- Column UNSContainer.CanonicalName extended to nvarchar (max) or clob respectively.
- Columns UNSContainer.cn extended to nvarchar(1024) or varchar2(1024) respectively.
- Column UNSContainer.DomainDisplayName shortened to nvarchar(128) or varchar2(128) respectively.
- Data type of column UNSContainer.ObjectGUID changed to nvarchar(256) or varchar2 (256) respectively.
- The column UNSGroup.IsApplicationGroup has been deleted.

Active Directory Module

- New column ADSDomain.ObjectSID.
- The column ADSContainer.IsAppContainer has been deleted.
- The column ADSGroup.IsAplicationGroup has been deleted.

Microsoft Exchange Module

- New table EX0OwaMailboxPolicy and new column EX0MailBox.UID_EX0OwaMailboxPolicy for mapping Outlook Web App mailbox policies.
- New column EX0MailBoxDatabase.IsRecovery for labeling as recovery database.

LDAP Module

- The column LDAPContainer.IsAppContainer has been deleted.
- The column LDAPGroup.IsAplicationGroup has been deleted.

SharePoint Module

- New column SPSRLAsgn.MatchPatternForMembership for mapping categories for SharePoint roles.

SAP R/3 User Management module Module

- New column SAPLicence.Country for mapping country surcharges.
- New column SAPLicence.SonderVersion for mapping special versions.

SAP R/3 Compliance Add-on Module

- The column SAPRCRange has been deleted.

Universal Cloud Interface Module

- New columns UCIItem.CanonicalName, UCIItem.DistinguishedName and UCIItem.ObjectGUID.

Identity Management Base Module

- New column DPRNameSpace.IsFilterDesignerEnabled for displaying compliance rules in the rule editor.
- New column Person.BadPasswordAttempts as failed login count.
- New column Person.BadPwdAnswerAttempts as failed answers to question count.
- New columns Person.Passcode and Person.PasscodeExpires for passcode usage.
- New column Person.PasswordLastSet for mapping the last password modification.
- Data type of column PersonPasswordHistory.XTouched changed to varchar(1) or varchar2(1) respectively.
- New column ShoppingCartPatternItem.ObjectKeyOrgUsedInAssign for specifying the role or organization to contain the assignment.
- New column PWODecisionHistory.IsFromDelegation for labeling whether the approval was met based on a delegation.
- New column PWODecisionSubMethod.RevisionNumber for specifying the revision number.
- New table QERWorkingMethod and new column PersonWantsOrg.UID_QERWorkingMethod for mapping instances of approval workflows.
- New table QERWorkingStep and new column PWOHelperPWO.UID_QERWorkingStep for mapping instances of approval steps.
- Data type of columns PersonWantsOrg.OrderDetail2 and ShoppingCartItem.OrderDetail2 changed to nvarchar(64) or varchar2(64) respectively.
- Columns QERCentralAccount.ColumnName and QERCentralAccount.TableName extended to varchar(30) or varchar2(30) respectively.

- Column QERCentralAccount.AccountName shortened to nvarchar(400) or varchar2(400) respectively.
- Columns QERMailAddress.ColumnName and QERMailAddress.TableName extended to varchar(30) or varchar2(30) respectively.
- Column QERMailAddress.UID_PK extended to varchar(200) or varchar2(200) respectively.
- Columns QERMailAddress.CompareValue and QERMailAddress.EmailAddress shortened to nvarchar(400) or varchar2(400) respectively.
- Column ESet.Ident_ESet extended to nvarchar(256) or varchar2(256) respectively.
- The column PWOHelperPWO.UID_PWODecisionStep has been deleted.
- The columns BaseTree.IsProviderRoot and BaseTree.UID_ProviderSyncServer have been deleted.

Attestation Module

- New column AttestationCase.UID_QERWorkingMethod for mapping instances of approval workflows.
- New column AttestationHelper.UID_QERWorkingStep for mapping instances of approval steps.
- New column PWODecisionStep.IgnoreNoDecideForPerson specifies whether the employee affected by this attestation instance may also approve it.
- The column AttestationHelper.UID_PWODecisionStep has been deleted.

Business Roles Module

- The column Org.UID_ProviderSyncServer has been deleted.

Synchronization template modifications

The following provides an overview of modified synchronization templates in One Identity Manager version 7.1.2. up to version 8.0.

- Non-functional changes do not necessitate the update of existing synchronization projects. In this case, you are dealing with minimal adjustments, such as changes to display names.
- Functions modification must be applied to existing synchronization projects so that all existing target system synchronizations can still be run without error. For more information, see Patches for synchronization projects on page 34.

Table 11: Synchronization template modifications

Module	Synchronization template	Type of modification	Patch ID
Azure Active Directory Module	Azure Active Directory synchronization	functional	VPR#27304
Active Directory Module	Active Directory synchronization	functional	VPR#27304, VPR#27457, VPR#27769, VPR#27997, VPR#28560_ ADS
Active Roles Module	Synchronize Active Directory Domain via Active Roles	functional	VPR#27304
Cloud Systems Management Module	Universal Cloud Interface synchronization	functional	VPR#27304, VPR#27371
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	new	
	Oracle E-Business Suite CRM data	new	
	Oracle E-Business Suite HR data	new	
	Oracle E-Business Suite OIM data	new	
Microsoft Exchange Module	Microsoft Exchange 2010 synchronization (deprecated)	functional	VPR#27304, VPR#27447, VPR#28904
	Microsoft Exchange 2010 synchronization (deprecated)	functional	VPR#27304, VPR#27447, VPR#28904
	Microsoft Exchange 2010 synchronization (v2)	new	VPR#28904
	Microsoft Exchange 2013_ 2016 synchronization (v2)	new	VPR#28904
G Suite Module	G Suite synchronization	new	

Module	Synchronization template	Type of modification	Patch ID
LDAP Module	AD LDS Synchronization	functional	VPR#27304
	OpenDJ Synchronization	functional	VPR#27304
IBM Notes Module	Lotus Domino synchronization	functional	VPR#27304, VPR#27769_NDO, VPR#28560_NDO
Exchange Online Module	Exchange Online synchronization (deprecated)	functional	VPR#27304
	Exchange Online synchronization (v2)	new	
SAP R/3 User Management module Module	SAP R/3 Synchronization (Base Administration)	functional	VPR#27289, VPR#27304, VPR#27769_SAP, VPR#28560_SAP
	SAP R/3 (CUA subsystem)	functional	VPR#27289, VPR#27304, VPR#28560_SAP
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	functional	VPR#27304
SAP R/3 Compliance Add-on Module	SAP R/3 authorization objects	functional	VPR#27539, VPR#27769_SAP, VPR#28560_SAP
SAP R/3 Structural Profiles Add-on Module	SAP R/3 HCM authentication objects	functional	VPR#27304
	SAP R/3 HCM employee objects	functional	VPR#27304
SharePoint Module	SharePoint synchronization	functional	VPR#27304
Universal Cloud	SCIM Connect via One	functional	VPR#27304,

Module	Synchronization template	Type of modification	Patch ID
Interface Module	Identity Connect For Cloud		VPR#27769_SCIM, VPR#27860, VPR#28560_SCIM
	SCIM synchronization	functional	VPR#27304, VPR#27769_SCIM, VPR#27860, VPR#28560_SCIM
Unix Based Target Systems Module	Unix Account Management	functional	VPR#27304
	AIX Account Management	functional	VPR#27304
SharePoint Online Module	SharePoint Online Synchronization	new	

Patches for synchronization projects

Patches for the following patch type are provided in One Identity Manager 8.0.

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

To adjust existing synchronization projects to One Identity Manager version 8.0, 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 8.0.

Patches for new function can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 8.0 for synchronization projects. Only patches created after version 7.1.2 are listed. For information about patches from earlier versions of One Identity Manager, see the respective release notes for each version.

TIP: Implement milestones first and then apply optional patches for new functions.

For more information, see Applying patches to synchronization projects on page 50.

Table 12: General patches

Patch ID	Patch	Description	Issue ID
VPR#27304	Method "UnmarkAsOut-standing"	Sets the method "UnmarkAsOut-standing" in provisioning workflows.	27304
	Milestone 8.0	Milestone for the context "DPR".	
	Milestone 8.0	Milestone for the context "One Identity Manager".	

Table 13: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "Azure Active Directory".	

Table 14: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#27457	Domain property object SID	Extends the One Identity Manager schema and the mapping for `ADSDomain` by the schema property `ObjectSID`.	27457
VPR#27769_ADS	Connection string conversion	Converts connection parameter names and values. This patch is applied during the One Identity Manager database update.	27769
VPR#28560_ADS	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context "Active Directory".	
VPR#27997	Change group membership sync	Extended the mapping "group" by additional virtual schema properties. This allows group memberships to be synchronized without having to find object SIDs through the global catalog. This is a patch for a new function. This patch can be applied optionally.	27997

Table 15: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "Active Roles".	

Table 16: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#27447	Use ObjectVersion to determine Microsoft Exchange version	Changing the "Organization" mapping to find the Microsoft Exchange version from the schema property `ObjectVersion`.	27447
VPR#28904	Add RemoteMailbox to ignore list	This patch modifies the member filter's excluded lists. Apply this patch if a Exchange hybrid environment exists but it not synchronized with One Identity Manager yet.	28904
	Milestone 8.0	Milestone for the context "Microsoft Exchange".	

Table 17: Patches for LDAP

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "LDAP".	

Table 18: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#27769_NDO	Connection string conversion	Converts connection parameter names and values. This patch is applied during the One Identity Manager database update.	27769
VPR#28560_NDO	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context "IBM Notes".	

Table 19: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#27769_SAP	Connection string conversion	Converts connection parameter names and values. This patch is applied during the One Identity Manager database update.	27769
VPR#27289	Create new	Extended mapping "Licencetype" to property	27289

Patch ID	Patch	Description	Issue ID
	rules on SAP licence	mapping rule for the schema property `Countries` and `SonderVersion`.	
VPR#28560_SAP	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context "SAP R/3".	

Table 20: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#28560_SAP	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context "SAP R/3 structural profile add-on".	

Table 21: Patches for SAP R/3 BI analysis authorizations

Patch ID	Patch	Description	Issue ID
VPR#28560_SAP	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context "SAP R/3 analysis authorizations add-on".	

Table 22: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
VPR#27539	Remove `SAPRCRange` mapping and extensions	Removes `SAPRCRange` from the schemas, mapping and workflows.	27539
VPR#27769_SAP	Connection string conversion	Converts connection parameter names and values. This patch is applied during the One Identity Manager database update.	27769
VPR#28560_	Display name	German display names of property mapping	28560

Patch ID	Patch	Description	Issue ID
SAP	conversion into English	rules and virtual schema properties are converted to English.	
	Milestone 8.0	Milestone for the context "SAP R/3".	

Table 23: Patches for SharePoint

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "SharePoint".	

Table 24: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#27769_SCIM	Connection string conversion	Converts connection parameter names and values. This patch is applied during the One Identity Manager database update.	27769
VPR#27860	Conversion of profile mapping	Changes the property mapping rules for the schema properties "id", "canonical name" and "distinguished name" to the new schema properties added for them in the One Identity Manager schema. This patch can only be applied in synchronization projects which contain the "Profiles" map. This patch is applied during the One Identity Manager database update.	27860
VPR#28560_SCIM	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context "SCIM".	

Table 25: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)

Patch ID	Patch	Description	Issue ID
VPR#27371	Pending change provisioning optimization	Provides a new variable and alters the scope.	27371

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "Universal Cloud Interface".	

Table 26: Patches for Unix

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "Unix".	

Table 27: Patches for the One Identity Manager connector

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "Database".	

Table 28: Patches for the CSV connector

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "CSV".	

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

One Identity Manager supports the following database systems:

- SQL Server
- Oracle Database

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 system	Windows operating system Following versions are supported: • Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later • Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 UNIX and Linux operating systems • Note the minimum requirements given by the operating system manufacturer for Oracle databases.
Related Applications	SQL Server • SQL Server 2016 Standard Edition, Service Pack 1 or later • SQL Server 2017 Standard Edition • Compatibility level for databases: SQL Server 2016 (130) • Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) NOTE: The SQL Server Enterprise Edition is recommended on performance grounds. Oracle Database • Oracle Database 12c Standard Edition or Enterprise Edition Version 12.1.0.2 and later The patch level differs depending on the system platform. NOTE: It strongly recommended you apply the patches for Oracle bugs 18097476 (Doc ID 1683819.1) and 19497286 (Doc ID 19497286.8) • Character set unicode (AL32UTF8) with the option “Oracle Text”; Parameter NLS_LENGHT_SEMANTICS with value "CHAR"

Minimum requirements for the service server

Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
operating system	Windows operating system Following versions are supported: • Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later • Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 Linux operating system • Linux operating system (64 bit), supported by the Mono project or Docker images provided by the Mono project.
Additional software	Windows operating system • Microsoft .NET Framework Version 4.5.2 or later NOTE: Microsoft .NET Framework version 4.6 is not supported. NOTE: Take the target system manufacturer's recommendations for connecting the target system into account. • Windows Installer Linux operating system • Mono 4.6 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 • Windows Vista with the current service pack • Windows 7 (32-bit or non-Itanium 64-bit) with the current service pack • Windows 8 (32-bit or 64-bit) with the current service pack • Windows 8.1 (32-bit or 64-bit) with the current service pack • Windows 10 (32-bit or 64-bit) with version 1511 or later
Additional software	• Microsoft .NET Framework Version 4.5.2 or later NOTE: Microsoft .NET Framework version 4.6 is not supported. • Windows Installer
Supported browsers	• 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 system	Windows operating system • Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later • Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 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 software	Windows operating system
	• Microsoft .NET Framework Version 4.5.2 or later
	NOTE: Microsoft .NET Framework version 4.6 is not supported.
	• Windows Installer
	• Microsoft Internet Information Service 7, 7.5, 8, 8.5 or 10 with ASP.NET 4.5.2 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
	• Mono 4.6 or later
	• NTP - Client
	• 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	Windows operating system • Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later • Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 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 software	Windows operating system
	• Microsoft .NET Framework Version 4.5.2 or later
	NOTE: Microsoft .NET Framework version 4.6 is not supported.
	• Windows Installer
	• Microsoft Internet Information Service 7, 7.5, 8, 8.5 or 10 with ASP.NET 4.5.2 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
	• Mono 4.6 or later

- NTP - Client
- 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 29: Supported data systems

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.
Connector for relational databases	Any relational databases supporting ADO.NET. NOTE: Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer.
Generic LDAP connector	Any LDAP directory server conforming to version 3. NOTE: Other schema and provisioning process adjustments can be made depending on the schema.
Web service connector	Any SOAP web service providing wsdl. NOTE: You can use the web service wizard to generate the configuration to write data to the web service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active Directory connector	Active Directory, shipped with Windows Server 2003 , Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2. Active Directory, supplied with Windows Server 2016, is only supported with a maximum functional level of Windows Server 2012 R2 at forest or domain level.
Microsoft Exchange	• Microsoft Exchange 2010 Service Pack 3 or later • Microsoft Exchange 2013 Service Pack 1 or later

Connector	Supported data systems
connector	• Microsoft Exchange 2016
SharePoint connector	• SharePoint 2010 • SharePoint 2013
SAP R/3 connector	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40 SR 2, 7.41, 7.50 • 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	• 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	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider
Mainframe connector	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 6.9 • Active Roles 7.0
Azure Active Directory connector	• Microsoft Azure Active Directory
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0.

Connector	Supported data systems
Exchange Online connector	• Microsoft Exchange Online
G Suite connector	• G Suite
Oracle E-Business Suite connector	• Oracle E-Business Suite System versions 12.1 and 12.2
SharePoint Online connector	• Microsoft SharePoint Online

Product licensing

This product does not require licensing.

Upgrade and installation instructions

NOTE: To install One Identity Manager 8.0 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:

- 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 8.0. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
  - Automatic software updating of version 7.0 to version 8.0 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.
  - Automatic software updating of version 7.1 to version 8.0 only works smoothly if the service pack 7.1.2 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 files, use the Software Loader.

  Future version 7.0 and 7.1 service packs will already contain the changes to these files and therefore, must not distributed separately.

To update an existing One Identity Manager installation to version 8.0

1. Update the administrative workstation, on which the One Identity Manager database schema update is started.
   a. Execute the file `Autorun.exe` from the root directory of the One Identity Manager installation medium.
   b. Change to the **Installation** tab. Select the edition you have installed and click **Install**.

      This starts the installation wizard.
   c. 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.
2. Shut down the One Identity Manager Service on the server that processes the database's direct queries (update server)
3. Create a backup of the One Identity Manager database.
4. If you are using an SQL Server database, set the compatibility level to "130"
5. Run the One Identity Manager database schema update.
   - Start the Configuration Wizard on the administrative workstation and follow the instructions.

6. Update the One Identity Manager Service on the update server.
    a. Execute the file `Autorun.exe` from the root directory of the One Identity Manager installation medium.
    b. Change to the **Installation** tab. Select the edition you have installed and click **Install**.

       This starts the installation wizard.
    c. 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.
    d. 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.
7. Start the One Identity Manager Service on the update server.
8. Update other installations on workstations and servers.

   You can use the automatic software update method for updating existing installations.
9. 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.
10. 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. For more information, see Applying patches to synchronization projects on page 50.

    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.

To update an application server to version 8.0

- 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 8.0

NOTE: If the Web Portal is connected through an application server, ensure that the application server is updated before the Web Portal.

- To update the Web Portal automatically, connect to the monitoring site `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 Manager web application to version 8.0

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

Applying patches to synchronization projects

CAUTION: **Patches do not change customizations in synchronization projects. This mean 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 necessary improvements for the synchronization project.
2. Check whether conflict 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.

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. Select the milestones to apply under **Available patches**.

   In the patch details view, all dependent patches are listed in the order in which they will be applied.

4. Click **Apply selected patches**.
5. Enter any user input as prompted.
6. Optional: Select the patches to apply for new functions under **Available patches**. Multi-select is possible.

   In the patch detail view, patches are listed in the order in which they will be applied.
7. Click **Apply selected patches**.
8. Enter any user input as prompted.
9. If necessary, 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:

- Synchronization template modifications on page 31
- Patches for synchronization projects on page 34

Verifying successful installation

To determine if this version is installed

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

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

  The following version number indicates that this module is installed.

Module	Version number
Exchange Hybrid Module	2017.0011.0004.0010
Microsoft Exchange Module	2017.0011.0004.0010

Module	Version number
SharePoint Online Module	2017.0011.0004.0004
All other modules	2017.0011.0004.0000

Additional resources

Additional information are available in:

- 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

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

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.

One Identity Manager Release Notes
Updated - December 2017
Version - 8.0