

One Identity Manager 8.0.1

Release Notes

March 2018

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
- One Identity Manager Composition API Object Model Documentation

About One Identity Manager 8.0.1

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

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 8.0.1 is a patch release with new functionality and improved behavior. See [Features](#) on page 2 and [Enhancements](#) on page 3.

Features

New features in One Identity Manager 8.0.1:

Basic functionality

- The new configuration parameter "Common\Jobservice\AutoCreateServerFromQueues" can be used to control whether Job server entries are created for unknown queues in the One Identity Manager database. The configuration parameter is set by default. This creates new job servers in the database when the One Identity Manager Service has queries for missing queues. If you do not want this functionality, disable the configuration parameter.
- The search index on the application server can be manually updated. The function "Update Index" is available in the application server to do this. You can choose whether all indexes or only modified indexes are updated.
- Database encryption uses RSA encryption with a key length of 3584 bits. Use the program Crypto Configuration to change an existing encryption.
 - ① **NOTE:** Columns with encrypted values like password columns, for example, have been extended in the One Identity Manager schema. If you have extended the One Identity Manager schema with custom columns for mapping encrypted value, these column must be also extended if necessary.

Web Portal

- Azure Active Directory OAuth Authentication is available for logging in to the Web Portal.

Target system connection

- Support for SharePoint 2016
- Support for Active Roles 7.2

- A schema editor has been integrated into the Synchronization Editor.
- Support for uninstalling the supplied BAPI from an SAP R/3 system.

Prerequisites:

- SAP NetWeaver Application Server version 7.00 or later and the SAP Add-On Assembly Kit 5.0 or later are installed in the SAP R/3 environment.
- The BAPI was installed with the Assembly Kit package.

See also:

- [Enhancements](#) on page 3
- [Resolved issues](#) on page 9
- [Schema changes](#) on page 27
- [Patches for synchronization projects](#) on page 32

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.0.1.

Table 1: General

Enhancement	Issue ID
Custom definitions can be used for prioritizing processes.	27204, 3774308
Support for deleting modules from a One Identity Manager database.	27876
If a process runs for more than 500 ms, the execution status "Processing" is display in Job Queue Info.	29064
Private key protection can be set up by configuring the One Identity Manager Service. If the key should not be protected, the key file is not moved to the user-related key container when the service is started.	29245
The path (execution target) is masked when the One Identity Manager Service is called.	28630, 4107917
Improved performance determining display columns of foreign key columns. The original object is taken into account when the permissions are tested. Only FK objects for this, the original object are displayed.	28427, 4074610, 4071727, 4100881, 4167180
Improved re-enabling of triggers and constraints.	28637, 4107215, 4109588

Enhancement	Issue ID
Data export in the Manager now additionally supports certain system tables.	29328, 4166103
Improved performance calculating responsibilities in the One Identity Manager.	29081, 29526, 4146692, 4183692
Process handling is interrupted during processing of DBQueue Processor triggers and constraints.	27486, 4191893
Custom password policies can be transported.	29241
The behavior of the procedures QBM_VForeignKeyRepairable, QBM_PForeignKeyWrongRepair and QBM_PForeignKeyWrongReport has been extended to include functionality for handling object keys with no restrictions in the table ValidDynamicRef but that reference a non-existent table.	27876
Improved logging for error 810029.	4194482, 4148032, 29571
<p>Handling of certificates for TLS encrypted email notifications can be configured over the configuration parameters "Common\MailNotification\AcceptSelfSignedCert" and "Common\MailNotification\AllowServerNameMismatchInCert". In the process component MailComponent, the desired behavior can be controlled with the parameter AcceptSelfSignedCert and AllowServerNameMismatchInCert.</p> <p>The option "None" under the configuration parameter "Common\MailNotification\TransportSecurity" has been extended. In the process component MailComponent, the desired behavior can be controlled with the parameter NoTransportSecurity. If the option "None" is set, connection to the SMTP server are not encrypted.</p> <p>All default processes for sending email have been assigned the parameters AcceptSelfSignedCert, AllowServerNameMismatchInCert, EnableSSL, NoTransportSecurity, StartTLS, StartTLSWhenAvailable as optional parameters.</p>	4211375, 4212295, 4215480, 4206033, 4223204, 29512
<p>i NOTE: These changes cause SSL and TLS server settings to be monitored more strictly. Therefore, it is imperative you check that the configuration parameter settings correspond to your environment, otherwise processes may not be executed correctly in certain circumstances.</p>	
A new server function "CSV script server" is available for the Job server. This can be assigned to a Job servers, which execute CSV import or exports using scripts.	4193949, 29558


Enhancement	Issue ID
The server function "CSV connector" is not automatically assigned to every new Job server anymore.	
To generate simple list reports, the process function ScriptComponent's CSVExport is used.	3993358, 28782
In the database search in the Manager in simple mode, the search term is automatically enclosed in asterisk (*).	4222855, 29596
Improved security when saving deferred operations. The system user context for deferred operations is always the current user.	29682

Table 2: General - Web Designer and Web Portal

Enhancement	Issue ID
The Web Designer configuration parameter "VI_ITShop_Employee_Preselec- ted" can be used to set whether the requester, if requesting for others, should be selected as recipient by default or not.	740767
Web Portal installation checks whether an application server with an installed search index has been configured.	29280
Improved performance for loading delegations in the Web Portal.	29414, 4183699- 1
Exporting a grid in the Web Designer is limited to 100 000 data sets. A message is displayed is the grid has more data sets.	28368, 4045185
Improved displaying of errors during debugging in the Web Designer. If data cannot be read due to access rights errors, an explicit message is displayed.	29385, 756599
The Web Designer Configuration Editor can now be opened with Microsoft Edge as well.	750374
When selecting an additional authentication module for the Web Portal, you can also select a space character.	742096
Improved representation and differentiating of read-only and write data in the Web Designer.	732447
Improved accessibility in the Web Portal.	749444
Improved layout in the Web Portal.	
Improvements in the Operations Support Web Portal.	
The path of a selected file is displayed again in the Web Designer.	4196410, 4201203, 29560

Enhancement	Issue ID
Improved performance calculating responsibilities in the One Identity Manager. The view QERVEditEmployee has been replaced by the view QER_VEditEmployee. If you use the view QERVEditEmployee in custom web projects, replace it with the view QER_VEditEmployee. Use the Web Designer's "Search and replace" function to do this. Then compile the web project.	29526, 4183692
Improved input options in the component VI_Edit_MultiValueProperty.	725139
Improved performance for deleting role memberships in the Web Portal.	4221646, 29629

Table 3: Target system connection

Enhancement	Issue ID
Support for Windows Server 2016 Active Directory domain functional level. A patch with the patch ID VPR#27583 is available for synchronization projects.	27583, 3942607
The option Only suitable for updates is enabled for the mapping "person" in Active Directory synchronization projects. A patch with the patch ID VPR#29360 is available for synchronization projects.	29360, 4179760
Improved security handling synchronization and provisioning processes.	27785
Comprehensive logging of error messages occurring during provisioning.	28825, 4105031
The SCIM connector allows differently constructed JSON objects for testing the endpoint configuration.	29076
Information about G Suite groups, products and SKUs is now displayed fully in the Manager.	28855
Patches that have not yet been applied are marked with  In the Synchronization Editor's patch view.	29261, 4075053
The revision filtering for synchronizing Exchange hybrid has been optimized.	29146
Extensions for supporting Exchange hybrid are now described in the One Identity Manager Administration Guide for Connecting to Microsoft Exchange.	
Improved reference resolution if more than root site with the same ID exists in a SharePoint environment. A patches with the patch IDs VPR#29240A and VPR#29240B are available for synchronization projects.	29240
Improved transfer of the validity period for SAP role assignments and memberships in structural profiles.	28031,

Enhancement	Issue ID
	4041294, 4054671
Synchronization engine messages are logged in more detail if the severity level "Trace" is set in the configuration file.	29400, 4129072
The columns PADEST and PASTANDORT are used in the display pattern for SAP printers.	29286
Maps for Notes domains and user accounts have been cleaned up. A patch with the patch ID VPR#29441 is available for synchronization projects.	29441
A synchronization project can be configuration for synchronizing different Oracle E-Business Suite systems. A patch with the patch ID VPR#29565 is available for synchronization projects.	29565
A wrapper package is made available to create a synchronization user with the required minimum permissions for synchronizing an Oracle E-Business Suite. A patch with the patch ID VPR#28876 is available for synchronization projects.	28876
Optimizing VI.DB for bulk processing of synchronization objects.	22785
Testing for uniqueness of Microsoft Exchange object aliases is now done across all objects.	29154
The script VI_PersonAuto_GetPropMappings has been renamed in TSB_PersonAuto_GetPropMappings and expanded by the function TSB_PersonAuto_GetColumnsWhereClause. The auxiliary script VI_PersonAuto_GetColumnsWhereClause has been deleted.	29210
The configuration parameters "TargetSystem\EBS\Accounts\PrivilegedAccount\SAMAccountName_Postfix" and "TargetSystem\EBS\Accounts\PrivilegedAccount\SAMAccountName_Prefix" have been deleted and replaced by the following configuration parameter: "TargetSystem\EBS\Accounts\PrivilegedAccount\AccountName_Postfix" and "TargetSystem\EBS\Accounts\PrivilegedAccount\AccountName_Prefix".	29562
Checks whether an application server supports full text search by search index.	25905

Table 4: Identity and Access Governance

Enhancement	Issue ID
Improved performance when querying delegations.	28964, 4071727
The documentation for inheriting company resource through system roles and	28312, 4057842

Enhancement	Issue ID
the effect of exclusion definitions has been comprehensively reworked (One Identity Manager System Roles Administration Guide).	
Improved performance loading attestation cases.	28796, 28966, 4100881, 4135798, 4183692
Improved performance making requests with the shopping cart.	29336, 29384, 4166207
Improved behavior for disabling and reenabling system roles.	29226, 29264, 4158272, 4159021
Improved performance renewing or canceling a request if the configuration parameter "QER\ITShop\DecisionOnInsert" is set.	29417, 4121616
Members of the chief approval team can make approval decisions for other approvers who have not responded to a query yet.	29323

See also:

- [Schema changes](#) on page 27
- [Patches for synchronization projects](#) on page 32

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.

- Archiving historical data using XML files (version 8.0.1 or later)
 - The following configuration parameters have been removed:
 - "Common\ProcessState\ExportPolicy\ExportPath",
 - "Common\ProcessState\ExportPolicy\ExportServer",
 - "ProcessInfoImport\ImportPath", "ProcessInfoImport\ImportServer",

"ProcessInfoImport\IgnoreDirectOperations" and "ProcessInfoImport".

- The option "FILE" has been removed in the configuration parameter "Common\ProcessState\ExportPolicy".
- The schedules "Export process information" and "Import process information" have been removed.
- The processes "VID_Export_ProcessInfo" and "VI_ProcessInfo_Import" have been removed.
- The process tasks "ExportProcessInfo" and "ImportProcessInfo" have been removed from the process component "ScriptComponent".

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)

NOTE: The tool "Oracle Data Migrator" is provided to help you convert database system. 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/>.

Resolved issues

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

Table 5: General

Resolved issue	Issue ID
The form "VI_HistoryDB_SourceDatabase_MasterData (FrmSourceDatabaseStammdaten)" shows empty user (DBUserName) and password (DBUserPwd) fields.	28906, 4125028
The export function in the Manager does not replace line feeds without a carriage return.	28977, 4122547
Master data forms in the Manager do not show the appropriate symbol for all changes.	29016, 4120015
Fallback to the configuration parameter "SysConfig\Logon\DefaultUser" whilst authenticating does not work.	29050, 4137430
In certain circumstances, unnecessary BLOBs are loaded when generating conditions are tested.	29093, 3859791
Changes to DialogUserInGroup raise the "DIALOG" semaphore too frequently.	29105, 4159711

Resolved issue	Issue ID
Subsequent calculations of inheritance are continued under the wrong GenProcID.	29132, 4156899
Parallel execution of QBM_PBrokerMessageSend can sometimes cause an error that irreparably damages the transaction.	25348, 4116732
Under SQL Server, it is possible to create new entries in QBMGuidReplace although GUIDReplace is already running.	28432, 4090349
If primary keys changed by migration, it might result in invalid references.	28614, 4079826
Download control throws an exception if the File name on client field remains empty.	28890, 4119141
The schedule start times are not logged in the database journal.	28924, 4136110
Entries in QBMElementAffectedByJob that result from deleting entries from many-to-many tables are created twice.	28944, 4136899
JobChain.LimitationWarning cannot be customized.	28946, 4135505
Reoccurring errors in the database journal.	28948, 4136642, 4141125, 4154532, 4147201, 4219304, 4206036, 4228965
Error creating a transport package if the time format was converted to "HH.mm".	28959, 4138380, 4210484
Error occurs importing your own filters that have been exported.	28994, 4121563
Wrong behavior of DialogColumn.IsNoAutoExtendPermissions. If this option is set for custom columns on a default table, permissions should not be assigned automatically.	29010, 4109829
There is no message when saving a report in the Report Editor, if permissions are missing.	29040, 4128282
Missing permissions for the database role "basegroup".	29054, 4134947

Resolved issue	Issue ID
The message Broker is always recreated when UID_Database is changed.	29102, 4159543
The condition (where clause) is not shown correctly when you change the filter modes.	29116, 4154252
Querying historical data takes a long time.	29130, 4157096
Compilation fails if request parameters are of type "Primary Key".	29133, 4135781
Under certain circumstances, the following error message appears whilst editing or displaying a mail template in HTML format in the mail template editor: Index was out of range Must be non-negative and less than the size of the collection.	29148, 4143404-1
External applications, started by the process component "CommandComponent", are not exited. The processes cannot be processed further.	29149, 4151840
Schema extensions cannot be assigned to an existing change label.	29153, 4164352
Insufficient permissions for SQL Server database users.	29158, 4165224
<p>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.</p> <p>All new installations and updates of version 8.0 after the 9th December 2017 are affected.</p> <p>This fix deals with the problem described in the knowledge article under https://support.oneidentity.com/kb/235185 .</p>	29170, 4170482-1
The process component SQLComponent only connects to the SQL Server 2016.	29177, 4163520
Assignments from the table QBMFileHasDeployTarget are not displayed in the Designer.	29190, 4164348
Tasks are not queued in the DBQueue if a front-end simulation that also created these tasks is running in parallel.	29195, 4162728
In certain circumstances, scheduled tasks are executed while the One Identity Manager is being updated with the Configuration Wizard.	29197
Recording B table views in the configuration buffer (QBMBufferConfig) does not work.	29198, 4142043
After changing the machine role for a custom file, the file is not distributed by	29208,

Resolved issue	Issue ID
automatic software distribution.	4166085
Error displaying change history for certain properties when connecting over the application server.	29214, 4155618
The HistoryDB Manager cannot be started over the Launchpad.	28909, 4124997
Tasks are not queued in the DBQueue if a front-end simulation that also created these tasks is running in parallel.	29195, 4162728
The options for assigning files to machine role are not shown correctly in then Software Loader.	29302, 4167290
DBTransporterCmd.exe runs as a 32-bit program.	29332, 4167225
The process component "MailComponent.SendRichMail" does not remove the lock from attachments it has utilized.	29352, 4183971
Users with "Read-only" permissions can display simple list reports in the Manager.	29283, 4165344, 4223969
Installation files, which are not required, are provided as MSI packages.	29122, 4156903
Default call statuses cannot be customized.	29353, 4188175
Automatic software update only partially works.	29182, 4164348, 4166640, 4150954, 4163316, 4162431, 4223947, 4221609
Error transporting schema extensions, which are assigned to a change label.	29308, 4180776, 4206307, 4214415
During migrating to One Identity Manager version 8.0, the script is entered in the column PriorityDefinition in all process steps for custom processes. Thus the priority for this process step cannot be set using the slide ruler subsequent to migration.	29365, 4189326
Error copying empty values from the result of an SQL query in the Object	29310,

Resolved issue	Issue ID
Browser.	4171762
Error logging in to the Designer with a system user without sufficient permissions.	29408, 4193830
One Identity Manager standard software cannot be assigned to user defined machine roles.	29419, 4193772
If files are deleted in a process step and place holders are used in the given files names, too many files may be lost in some cases.	29407
Inconsistent module assignment of Windows PowerShell components.	29411, 4193772
Error encrypting passwords in the One Identity Manager database.	29343, 4201181
Some time zones are not assigned to a country.	29451, 4161544
Error handling processes if processes are involved, that use the process task with JobTask.IsExclusivePerObject='1' (for example, provisioning processes).	29458, 4169048, 4172806, 4204568
Incorrect determination of table names in consistency checks.	29482, 4204124
Under certain circumstances, a system configuration transport might causes double entries in the table DialogMultiLanguage.	4201862, 4218254, 29492
Attachments in EML files created by the "DebugMailPlugin" lose their original names.	4200044, 29503
The function QER_FGIAdminUnitForPerson does not the columns DialogCountry.IsInUse and DialogState.IsInUse into account when calculating work hours.	4188488, 29505
Error executing dialog method on objects that are selected with multi-select.	4197196, 29516
If a priority definition is changed or deleted on a process step, the process step is generated with the previously defined priority anyway.	4198425, 29561, 29568
Error transporting schema changes because DialogColumn.UID_DialogColumn is not unique in the databases which are involved.	4216079, 29587
Error transporting the system configuration because dependencies are not taken into account.	4201862, 29598

Resolved issue	Issue ID
Deep links for opening objects do not work in the Manager web application anymore.	4189352, 29613
The context menu for nodes in the Designer's navigation view shows the wrong entries.	4204470, 29618
Error selecting an object from a menu containing many-to-many table objects.	4221974, 29420
The dialog Change history does not show the time in local format.	4208320, 29446
Replacing process parameter for an encrypted database fails.	4216756, 29633
Disabled tasks are also displayed in the Manager's task view.	4203208, 29644
Triggers are not generated for the configuration buffer.	4234683, 29664

Table 6: General - Web Designer and Web Portal

Resolved issue	Issue ID
The progress bar for attestations stays at 0% for the chief approval team.	28980, 4061270-1
Certain ObjectWalker expressions cause compiler errors.	28928, 4135787
Error in the callback response in Web Designer runtime.	29009, 4148377
Inappropriate indexing in component "VI_Roles_Membership", Collection "PersonObjects".	29104, 4154312-1
List reports with more than 32 columns cannot be displayed in the Web Portal.	29268, 4170675
Display is inconsistent when the One Identity Password Manager is opened from the Web Portal.	29035, 4103198
Error in the Web Portal when a product is unsubscribed immediately after successfully unsubscribing a different one.	29325, 4179656
Menus and views are displayed incorrectly in the Web Portal if at least one of the configuration parameters "QER\CalculateRiskIndex", "QER\Policy" or "QER\ComplianceCheck" is disabled.	29388, 29452,

Resolved issue	Issue ID
	760379, 4184811, 4189123
Sub categories and products of a service category are displayed incorrectly if the service category was opened using a bookmark.	29418, 4192045
Error in the wizard for adding new web projects and new modules in the Web Designer.	29347, 4188403- 1
Error in the view Pending requests in the Web Portal by double-clicking on the Status button.	29196, 4165931
Error compiling a custom module in debug mode in the Web Designer.	28763, 4117298
Login with single sign-on is not possible if an additional authentication module is given.	4182868, 4204172, 4217515, 4223508, 4209301, 29096, 29460
Too many vertical scrollbars are shown in the Web Portal when the detail content view of the main content view.	29478, 4196401
Internal server error if, shortly after saving a pending attestation in a briefly opened Yes/No dialog box, Yes is clicked again.	4121556- 1, 29423
in the "HierarchyTableHelper", a Where clause is built with "isnull" and "not in". This combination sometimes causes longer runtimes.	4206323, 4206323, 29530
The component "VI_Edit_View_URL" does not show any links.	4156154, 29082
The function QER_FGIPW00rderPerson is only called without person.	4196689, 29529
Report parameter display names are not always displayed in the Web Portal. i NOTE: The solution to this problem only works for parameters of newly created report subscriptions.	4194362, 29552
If the button for adding a new employee through an extension in module VI_Employee_Overview is deleted, no more data is displayed on the master data page.	4188140, 29584

Resolved issue	Issue ID
Cannot export views with Data Source=Collection.	4181271, 4206038, 29278
Error create attestation policies in the Web Portal.	4206458, 29651
Display error in the Operations Support Web Portal.	4183038, 29467

Table 7: Target system connection

Resolved issue	Issue ID
Error in script ADS_GenerateHomeAndProfileEvent.	28884, 4112445
Diverse errors executing MaintainOtherSID due to unresolvable Active Directory group memberships.	29115, 29209, 4150968, 4170066, 4170021, 4220273, 4228975
Error synchronizing Active Directory site servers. A patch with the patch ID VPR#29299 is available for synchronization projects.	29299, 4183020
In certain circumstances, the option Change password the next time you log in is reset although no changes have been made to the password by the Active Directory user.	29301, 4168196
The Customizer prevents ADSDomain.MaxPasswordAge being set to "0" and ADSDomain.MinPasswordAge to "1".	29303, 4177588
You cannot set ADSDomain.MaxPasswordAge to the value "0". A patch with the patch ID VPR#29318 is available for synchronization projects.	29318
Changes to ADGroup.AllowWriteMembers are not provisioned. A patch with the patch ID VPR#29122 is available for synchronization projects.	29410, 4176358
It is apparently not possible to add an administrator to a distribution group.	29434, 4171655, 4223916
Error editing Active Directory groups in the Manager web application.	4173501, 4210457, 29074

Resolved issue	Issue ID
Incorrect entries in DPRMembershipAction when objects are deleted.	28879, 29232, 4102450
The connection to the target system cannot always be saved if a value in a script variable is changed.	28950, 4046109
Error message System.FormatException: Input string was not in a correct format. sometimes appears if logging provisioning of objects with curly brackets in their names, with the severity level "Trace".	28993, 4139793, 4214700
Schedules, which have been changes to "Every minute" in the Designer, are not displayed properly in the Synchronization Editor.	29068, 4134900
Error using "\$\$" in a database user's password if the One Identity Manager database is encrypted.	28556, 4101908, 4174814, 4174814, 4208245
Error solving FK properties by using One Identity Manager connectors.	29271, 4179959
Error in provisioning processes in step "Check Properties" if an empty value is passed.	29479, 4170216
Entries in the table DPRProjectionStartInfo are deleted when synchronization projects imported.	4212736, 29554
Improved error messaging for schema errors in the LDAP connector.	28620, 4087587
Error reading attributes with type=certificate.	28877, 4115139
Error in the LDAP connector when emptying or deleting a value of a "Binary" field.	29159, 4156414
NullReferenceException resolving references on the IBM Notes Server.	28868, 4128243
Revision counters are not examined and saved during synchronization with IBM Notes.	28917
A patch with the patch ID VPR#28917 is available for synchronization projects.	
Various error handling SAP schema extensions: <ul style="list-style-type: none"> Property definitions on schema types do not appear in the extended schema and, therefore, cannot be used in the mapping. Properties from the Properties Block are not read in when a synchron- 	26717, 29257, 3683936, 4150766

Resolved issue	Issue ID
ization is reloaded.	
SAPComPhone.PhoneType does not alter correctly.	28818, 4073192
Error synchronizing SAP authorization objects if more than 16, 777, 216 data sets per table must be processed.	28875, 4120295
Incorrect resolution of data in the SAP connector if the loading buffer's threshold is exceeded.	28895, 4121833
There is no filtering of SAP personnel planning data about an employee when it is loaded with BAPI_EMPLOYEE_GETDATA. A patch with the patch ID VPR#28927 is available for synchronization projects.	28927, 4145642, 4151642, 4208404
Too many user groups are displayed on the master data form for SAP user accounts.	29012, 4114977
The GenProcID is not passed correctly when calculating SAPUserInSAPRole.	29034, 4073967
UID_PersonHead is not deleted if the department in SAP R/3 loses its manager.	29046, 4088264
The parameter list is not available when an SAP user account is created.	29281, 4114864
The process step Check User already exists in the process SAP_SAPUserParameter_Insert/Update is not generated.	29282, 4114864
Error provisioning memberships in SAP groups or profiles.	29377, 4106789
Error synchronizing group memberships for cloud applications. A patch with the patch ID VPR#29454 is available for synchronization projects.	29454
The RACF connector sometimes sets the search area for RacfProfileType objects incorrectly.	4199446, 29522, 29574
Error reloading objects of type "Dataset" in the RACF connector.	4199376, 29624
If a password has been changed in LDAP, the RACF connector does not mark the password as expired.	4219465, 29684
When objects are deleted from target systems, the corresponding entries in the table DPRMemberShipAction are not removed. This causes provisioning errors.	27461, 3888825, 3792817,

Resolved issue	Issue ID
	3953699
Translations of mapping rules for categories cannot be maintained in the Manager.	4180537, 4198536, 4189336, 4212811, 4216983, 29071
Passwords are visible in the synchronization log if modified properties and values are logged. A patch with the patch ID VPR#29603 is available for synchronization projects.	4213531, 29603
Error provisioning if a rule filter has been set.	4062186, 29612
Error creating a synchronization project for Exchange Online if the password contains "\$".	4201175, 29623
Only SAP transactions, which maintain a translation in the synchronization user's login language, are synchronized. A patch with the patch ID VPR#29547 is available for synchronization projects.	4210568, 29547
If a date is entered in a schema extension file for an SAP R/3 synchronization project as an input parameter for a function, the date is converted incorrectly.	4207491, 29589
Assignment of the same attributes with different values are not loaded during synchronization of security attribute assignments to E-Business Suite user accounts. A patch with the patch ID VPR#29543 is available for synchronization projects.	29543
User account cannot be added because too many schema properties are labeled as mandatory properties. A patch with the patch ID VPR#29528 is available for synchronization projects.	29528
Error provisioning if SAPUser.InActivePWD is enabled. The error only occurs in SAP systems of version SAP NetWeaver Application Server 7.10 or later. A patch with the patch ID VPR#29614 is available for synchronization projects.	29614

Table 8: Identity and Access Governance

Resolved issue	Issue ID
Rule groups can be saved without a name.	28867

Resolved issue	Issue ID
<p>i NOTE: For existing installations: The rule group's name is now a compulsory field. Check by running the consistency check "Mandatory field check" on your existing data.</p>	
Write error for compliance rules in the Customizer.	28974, 4119536
In certain circumstances, an EX step is not triggered when the event is canceled.	28976, 4113159
The column BaseTree.FullPath is too short.	29003, 4115743, 4138341
The configuration parameter "Common\ProcessState\UseGenProcIDFromPWO" allows you to specify whether the GenProcID of an IT Shop request is kept for the entire approval process period or whether a new GenProcID is used for each approval decision.	29206, 4156899
The statistic definition AttestationDecisionsInOverLimit_By_Department contains incorrect JOIN queries.	29284, 4178731
The ViewAddOn UNSAccountInUNSGroup EX0 prevents attestation of memberships in system entitlements.	29358, 29398
<p>i NOTE: The ViewAddOn has been deleted. Members of Microsoft Exchange mailboxes, mail users and mail contacts are not mapped in the Unified Namespace anymore. Mailboxes, mail users and mail contacts are still mapped in the Unified Namespace.</p> <p>If you required compliance rule for authorizing Microsoft Exchange objects, you can formulate them as SQL query for the underlying Active Directory objects.</p>	
Recalculation of PWOHelperPWO.UID_PWORulerOrigin is missing, if delegation is ended or broken off when an approval procedure for another request is running.	29242, 4159227
The report "VI_ComplianceRule_Overview_UID_RolesProfAuth" does not show the origin of rule violations caused by SAP functions.	29243, 4148586
Error canceling or renewing requests if the valid from date is older than the product's validity period will allow.	29378, 4188420
Error calculating which manager in a role hierarchy is responsible, if the option Block inheritance is set.	29381, 4184702

Resolved issue

Issue ID

- i** **NOTE:** In hierarchies with bottom-up inheritance, the manager's responsibility is changed by this. The following applies in every hierarchy:
- The manager of a parent role is responsible for all child roles, irrespective of the direction of inheritance.
 - The option **Block inheritance** has no influence on the calculation of the manager responsible.

In certain circumstances, incorrect data is saved when changes to employees master data in the Manager are saved.	29387, 4157086
Error deleting employees with dependencies over the object layer.	4173609, 29461
The repair script for the consistency test "Product assignment without a request" does not work.	4208564, 29538
Error setting up IT Shop using a shopping center template if the configuration parameter "Software\Application" is not set.	4187539, 29599
Error in the procedure QBM_PDeleteDeep under Oracle Database.	2657573, 27643
The field Spare field no. 06 is missing on the tab Additional Information on the Request Details form.	4231273, 29637
The view QERVPersonAndAERoles returns data sets with identical primary keys that occur more than one.	4206458, 29671

See also:

- [Schema changes](#) on page 27
- [Patches for synchronization projects](#) on page 32

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-	3209411,

Known Issue	Issue ID
CommonWaitForCompiler" is immediately queued in the DBQueue. If 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 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
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. 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.	3372460, 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.	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
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	28373, 4081234

Known Issue	Issue ID
database cannot be compiled.	
Error resolving events on a view that does not have a UID column as a primary key. 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 a rudimentary 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 schema.	4206673, 4206673, 29535

Table 10: Web Designer and Web Portal

Known Issue	Issue ID
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
An empty page is displayed in the Internet Explorer if the Operations Support Web Portal is opened with the URL. The Operations Support Web Portal is supposed to be run on an intranet site and the setting is set on the web server. Solution: Extend the section <system.webServer> in the Web Portal's configuration file (web.config). Enter an attribute or compatibility mode. <system.webServer> ... <httpProtocol> <customHeaders> ... <add name="X-UA-Compatible" value="IE=11" /> ... </customHeaders> </httpProtocol>	750376

Known Issue	Issue ID
</system.webServer>	
If a new report is added, the report parameters are shown with the wrong names. Solution: Will be available in One Identity Manager version 8.0.2.	4194362, 29685

Table 11: Target system connection

Known Issue	Issue ID
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: <ul style="list-style-type: none"> • 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. 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
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. <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. 	3777857, 27359

Known Issue	Issue ID
<ul style="list-style-type: none"> 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 method "SetPassword" is, therefore, not available.</p> <p>The process step "AdhocProjection" fails with the message:</p> <pre>[System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKNOWNNAME)).</pre>	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>	3923873, 3932523, 27687
<p>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.</p>	28137
<p>Error in IBM Notes connector (Error getting revision of schema type ((Server))).</p> <p>Probable cause: The IBM Notes environment is 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, 4207491
Cause: The function "BAPI_EMPLOYEE_GETDATA" is always executed with the current date and therefore, changes are taken into account on 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. 	
If an employee's central password is used as the password for their user accounts, the password is not transferred to the password history of each user account. Therefore, reuse of the password cannot be prevented if the password is changed manually later.	29605
Cause: An employee's central password is an encrypted value that can only be entered in the password history when it is assigned to an employee.	
Recommendation:	
<ul style="list-style-type: none"> • Only use the employee's central password for the user accounts. Changes to the password are saved in the employee's password history. - OR - • Only make changes to the passwords directly in the user accounts. This saves the password modifications in the user account's password history. 	
Errors publishing group memberships if there are memberships that are not mapped.	4210722, 29691
Solution: Will be available in One Identity Manager version 8.0.2.	
The options Home address and Default address can be disabled, although	4205200,

Known Issue	Issue ID
only an email address is assigned to the SAP user account. Solution: Will be available in One Identity Manager version 8.0.2.	29700

Table 12: 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 an 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
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

Schema changes

The following provides an overview of schema changes from One Identity Manager version 8.0 up to version 8.0.1.

Configuration Module

- Data type changed and column DialogDatabase.PublicKey extended to varchar(671) or varchar2(671) respectively.
- Data type changed and columns DialogHistoryDB.ConnectionString and QBMPwdPolicy.DefaultInitialPassword extended to varchar(606) or varchar2(606) respectively.

- The following columns have been extended to varchar(606) or varchar2(606) respectively.

Table	Column
DialogWebService	ProxyPassword
DialogWebService	UserPassword
QBMServer	SRVAccount
QBMServer	SRVAccountDomain
QBMServer	SRVAccountPwd

- New column DialogSystemObject.UID_DialogSystemObject.
- New column QBMV3rdPartyLicence.UID_QBMV3rdPartyLicence.
- New column QBMVCustomInfo.UID_QBMVCustomInfo.
- New column QBMVSystemInfo.UID_QBMVSystemInfo.
- New column QBMVTableEventChain.UID_QBMVTableEventChain.

Target System Base Module

- Column UNSAccountB.Password extended to varchar(606) or varchar2(606) respectively.
- Column UNSContainer.cn extended to nvarchar(1024) or varchar2(1024) respectively.

Azure Active Directory Module

- Column AADUser.Password extended to varchar(606) or varchar2(606) respectively.

Active Directory Module

- New column ADSDomain.msDSExpirePasswdOnSCardOnlyAcc for enabling forwarding of expiring NTML keys.
- Column ADSAccount.UserPassword extended to varchar(606) or varchar2(606) respectively.

Cloud Systems Management Module

- Column CSMUser.Password extended to varchar(606) or varchar2(606) respectively.

Microsoft Exchange Module

- Column ADSDomain.EX0UserPassword extended to varchar(606) or varchar2(606) respectively.

Exchange Online Module

- Column O3EMailUser.Password extended to varchar(606) or varchar2(606) respectively.

G Suite Module

- Column GAPUser.Password extended to varchar(606) or varchar2(606) .

IBM Notes Module

- The following columns have been extended to varchar(606) or varchar2(606) respectively.

Table	Column
NDOCertifier	Password
NDOServer	Password
NDOUser	InternetPassword
NDOUser	Password
NDOUser	PasswordInitial

LDAP Module

- Column LDAPAccount.UserPassword extended to varchar(606) or varchar2(606) respectively.
- Column LDAPContainer.EX0UserPassword extended to varchar(606) or varchar2(606) respectively.

SAP R/3 User Management module Module

- Column SAPUser.Password extended to varchar(606) or varchar2(606) .

Universal Cloud Interface Module

- Column UCUser.Password extended to varchar(606) or varchar2(606) respectively.

Identity Management Base Module

- The following columns have been extended to varchar(400) or varchar2(400) respectively.

Table	Column
AERole	FullPath
BaseTree	FullPath
Department	FullPath
ITShopOrg	FullPath
ITShopSrc	FullPath
Locality	FullPath
ProfitCenter	FullPath

- Column DelegableItem.DisplayValue shortened to nvarchar(128) or varchar2(128) respectively.
- Column DelegableItem.FullPath shortened to nvarchar(400) or varchar2(400) respectively.
- Column Person.CentralPassword extended to varchar(606) or varchar2(606) respectively.

Compliance Rules Module

- Column NonCompliance.FullPath extended to nvarchar(400) or varchar2(400) respectively.

Business Roles Module

- Column Org.FullPath extended to nvarchar(400) or varchar2(400) respectively.

System Roles Module

- The table RMSVSEtHasEntitlementMNT has been deleted.

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 to version 8.0.1. Apply the patches to existing synchronization projects. For more information, see [Applying patches to synchronization projects](#) on page 52.

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 32.

Table 13: Modification overview

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	none
Cloud Systems Management Module	Universal Cloud Interface synchronization	none
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	changed
	Oracle E-Business Suite CRM data	none
	Oracle E-Business Suite HR data	none
	Oracle E-Business Suite OIM data	none
Microsoft Exchange Module	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (v2)	none
	Microsoft Exchange 2013_2016 synchronization (v2)	none
G Suite Module	G Suite synchronization	none
LDAP Module	AD LDS Synchronization	none
	OpenDJ Synchronization	none
IBM Notes Module	Lotus Domino synchronization	changed
Exchange Online Module	Exchange Online synchronization (deprecated)	none

Module	Synchronization template	Type of modification
	Exchange Online synchronization (v2)	none
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	changed
	SAP R/3 HCM employee objects	changed
SharePoint Module	SharePoint synchronization	none
SharePoint Online Module	SharePoint Online synchronization	changed
Universal Cloud Interface Module	SCIM Connect via One Identity Connect For Cloud	changed
	SCIM synchronization	changed
Unix Based Target Systems Module	Unix Account Management	none
	AIX Account Management	none

Patches for synchronization projects

The following is a list of all patches provided in One Identity Manager 8.0.1 for synchronization projects. 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.

For more information, see [Applying patches to synchronization projects](#) on page 52.

Table 14: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#27583	Support for domain functional levels 2016	Mapping of schema class domainDNS extended by the schema property msDF-ExpirePasswordsOnSmartCardOnly Accounts. Therefore, domain	27583

Patch ID	Patch	Description	Issue ID
		functional levels 2016 are supported.	
VPR#28863	Correction of patched synchronization projects	Corrects small differences between new synchronization projects and synchronization projects that have had patches applied to them. This patch is applied during the One Identity Manager automatic update.	28863
VPR#29299	Corrects Active Directory site handling	Corrects import of Active Directory sites and child machines.	29299
VPR#29318	Set and remove maxPwdAge in domains	Corrects operation for resetting if maxPwdAge is set to "never".	29318
VPR#29360	Avoid using employee mapping on insert	Marked employee mapping with "Only suitable for updates".	29360
VPR#29410	Mapping of schema property ADGroup.AllowWriteMembers	Inserts a property mapping rule for the schema property AllowWriteMembers in the group map. This patch is applied during the One Identity Manager automatic update.	29410
VPR#29603_ ADS	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system. This patch is applied during the One Identity Manager automatic update.	29603

Table 15: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#29318	Set and remove maxPwdAge in domains	Corrects operation for resetting if maxPwdAge is set to "never".	29318

Table 16: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#28876	Connection parameters extended	The connection parameters have been extended so that you can enter the user package for user account operations or a wrapper package.	28876

Patch ID	Patch	Description	Issue ID
VPR#29528	Changes the definition of mandatory properties.	Updates the target system schema and corrects the definition of mandatory properties for adding new user accounts. This patch is applied during the One Identity Manager automatic update.	29528
VPR#29543	Updates the target system schema.	Updates the target system schema for synchronizing security attribute assignments with different values to user accounts. This patch is applied during the One Identity Manager automatic update.	29543
VPR#29565	Supplies variables for connection parameters	Connection parameters are supplied as variables. This patch is applied during the One Identity Manager automatic update.	29565
VPR#29603_ EBS	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system. This patch is applied during the One Identity Manager automatic update.	29603

Table 17: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#28917	Changes the revision counter	Changes the revision counter. A new virtual schema property is used. This patch is applied during the One Identity Manager automatic update.	28917
VPR#29441	Property mapping rule corrections	Minor corrections of property mapping rules in "Domain" and "Person" mappings	29441
VPR#29603_ NDO	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system. This patch is applied during the One Identity Manager automatic update.	29603

Table 18: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#29603_SAP	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system. This patch is applied during the One Identity Manager automatic update.	29603
VPR#29614	Corrected schema property vrtInactivePwd	Corrected the definition of the schema property vrtInactivePwd. This patch is applied during the One Identity Manager automatic update.	29614

Table 19: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#28927	Changed mapping for the employees' central SAP user account.	Corrects how to determine employees' SAP user account (USERID) and e-mail address (EMAILADDRESS)	28927

Table 20: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
VPR#29547	Updates the target system schema.	Updates the target system schema for synchronizing SAP transactions irrespective of how the translation is maintained. This patch is applied during the One Identity Manager automatic update.	29547

Table 21: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#29240A	Corrects errors in the reference resolution, part 1	Deletes all property mapping rules and object matching rules that web.ID uses for resolving references or matching, respectively. Prerequisite for patch "VPR#29240B". This patch is applied during the One Identity Manager automatic update.	29240

Patch ID	Patch	Description	Issue ID
VPR#29240B	Corrects error resolving references, part 2	Creates new property mapping rules that use Web.Url for resolving references. Depends on patch "VPR#29240A". This patch is applied during the One Identity Manager automatic update.	29240

Table 22: Patches for the SCIM interface (Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#29454	Change group membership types	Inserts a new property mapping rule for the group membership's type.	29454
VPR#29603_SCIM	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system.	29603

Patches in One Identity Manager version 8.0

Table 23: General patches

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

Table 24: Patches for Azure Active Directory

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

Table 25: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#27457	New	Extends the One Identity Manager schema and	27457

Patch ID	Patch	Description	Issue ID
	schema property for domains	the mapping for ADSDomain by the schema property ObjectSID.	
VPR#27769_ ADS	Converts connection parameters	Converts connection parameter names and values. This patch is applied during the One Identity Manager automatic update.	27769
VPR#28560_ ADS	Converts German display names	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	Changes group membership mapping	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 26: Patches for Active Roles

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

Table 27: 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	Adds RemoteMailbox to the excluded list	This patch modifies the member filter's excluded lists. Apply this patch if an Exchange hybrid environment exists but it not synchronized with One Identity Manager yet.	28904
	Milestone 8.0	Milestone for the context "Microsoft Exchange".	

Table 28: Patches for LDAP

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

Table 29: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#27769_ NDO	Converts connection parameters	Converts connection parameter names and values. This patch is applied during the One Identity Manager automatic update.	27769
VPR#28560_ NDO	Converts German display names	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 30: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#27769_ SAP	Converts connection parameters	Converts connection parameter names and values. This patch is applied during the One Identity Manager automatic update.	27769
VPR#27289	Create new rules on SAP licence	Extended mapping "Licencetype" to property mapping rule for the schema property Countries and SonderVersion.	27289
VPR#28560_ SAP	Converts German display names	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 31: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#28560_ SAP	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context "SAP R/3 structural profile add-on".	

Table 32: Patches for SAP R/3 BI analysis authorizations

Patch ID	Patch	Description	Issue ID
VPR#28560_SAP	Converts German display names	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 33: 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	Converts connection parameters	Converts connection parameter names and values. This patch is applied during the One Identity Manager automatic update.	27769
VPR#28560_SAP	Converts German display names	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 34: Patches for SharePoint

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

Table 35: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#27769_ SCIM	Converts connection parameters	Converts connection parameter names and values. This patch is applied during the One Identity Manager automatic 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 automatic update.	27860
VPR#28560_ SCIM	Converts German display names	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 36: 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
	Milestone 8.0	Milestone for the context "Universal Cloud Interface".	

Table 37: Patches for Unix

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

Table 38: Patches for the One Identity Manager connector

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

Table 39: 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: <ul style="list-style-type: none">• 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 of operating system vendors for Oracle databases and SQL Server 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_LENGTH_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: <ul style="list-style-type: none"> • 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


	<ul style="list-style-type: none"> Windows Server 2012 R2 Windows Server 2016 <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 software	<p>Windows operating system</p> <ul style="list-style-type: none"> Microsoft .NET Framework Version 4.5.2 or later <p>i NOTE: Microsoft .NET Framework version 4.6 is not supported.</p> <p>i NOTE: Take the target system manufacturer's recommendations for connecting the target system into account.</p> <ul style="list-style-type: none"> Windows Installer <p>Linux operating system</p> <ul style="list-style-type: none"> 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	<p>Windows operating system</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Microsoft .NET Framework Version 4.5.2 or later <p>i NOTE: Microsoft .NET Framework version 4.6 is not supported.</p> <ul style="list-style-type: none"> Windows Installer
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 system	<p>Windows operating system</p> <ul style="list-style-type: none">• 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 <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 4.5.2 or later <p> NOTE: Microsoft .NET Framework version 4.6 is not supported.</p> <ul style="list-style-type: none">• Windows Installer• Microsoft Internet Information Service 7, 7.5, 8, 8.5 or 10 with ASP.NET 4.5.2 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


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	<p>Windows operating system</p> <ul style="list-style-type: none"> • 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 <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 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 40: Supported data systems

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.

Connector	Supported data systems
Connector for relational databases	<p>Any relational databases supporting ADO.NET.</p> <p>i NOTE: Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer.</p>
Generic LDAP connector	<p>Any LDAP directory server conforming to version 3.</p> <p>i NOTE: Other schema and provisioning process adjustments can be made depending on the schema.</p>
Web service connector	<p>Any SOAP web service providing wsdl.</p> <p>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.</p>
Active Directory connector	<p>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.</p>
Microsoft Exchange connector	<ul style="list-style-type: none"> • Microsoft Exchange 2010 Service Pack 3 or later • Microsoft Exchange 2013 Service Pack 1 or later • Microsoft Exchange 2016
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 S/4HANA On-Premise-Edition
Unix connector	<p>Supports the most common Unix and Linux derivatives. For more information, see the Authentication Services specifications.</p>
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

Connector	Supported data systems
	<ul style="list-style-type: none"> • 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 • Active Roles 7.0 • Active Roles 7.2
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

Product licensing

This product does not require licensing.

Upgrade and installation instructions

NOTE: To install One Identity Manager 8.0.1 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:

- 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 8.0.1. Otherwise the schema update cannot be completed successfully.

- Note the following for automatic software updating:

- Automatic software updating of version 7.0 to version 8.0.1 only works smoothly if the service pack 7.0.3 is installed. In addition, the files VI.Update.d11 and JobService.d11 must be installed.

Request the files VI.Update.d11 and JobService.d11 from the support portal.

To distribute the file, use the Software Loader.

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

- Automatic software updating of version 7.1 to version 8.0.1 only works smoothly if the service pack 7.1.3 is installed.

To update an existing One Identity Manager installation to version 8.0.1

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. Complete the One Identity Manager Service on the 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 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 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. 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_Shell has been started successfully.

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

For more information, see [Applying patches to synchronization projects](#) on page 52.

To update an application server to version 8.0.1

- 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 8.0.1

- ① **NOTE:** As from version 7.1. and later, the Web Portal requires an application server with a search service installed on it. For more information, see the document *Web Designer and Web Portal Changes* and the *One Identity Manager Installation Guide*.
- ① **NOTE:** Ensure that the application server is updated before you install 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 Operations Support Web Portal to version 8.0.1

1. Copy the contents of the folder `Modules\QER\dvd\AddOn\Operations Support Web Portal` to the installation directory for the Operations Support Web Portal, for instance `OperationSupport`.
2. Copy the following file in the folder `bin` into the Web Portal application install directory.
 - `Modules\QER\install\bin\QER.WebRuntime.WebApi.dll`
 - `Modules\QBM\install\bin\QBM.CompositionApi.Web.dll`

To update the Manager web application to version 8.0.1

1. Uninstall the 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 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 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 patches to apply under **Available patches**. Multi-select is possible.
In the patch detail view, 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. If necessary, use the patch log to check whether customization need to be reworked.
7. If required, rework customizations in the synchronization configuration.
8. Run a consistency check.
9. Simulate the synchronization.
10. Activate the synchronization project.
11. Save the changes.

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

For more detailed information about updating synchronization projects, see the One Identity Manager Target System Synchronization Reference Guide.

See also:

- [Modified synchronization templates](#) on page 31
- [Patches for synchronization projects](#) on page 32

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 version number 2017.0011.0004.0100 for all modules and the application version 8.0 2017-11-04-097 indicate that this version is installed.

This service pack updates all files that shipped with One Identity Manager 8.0.

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

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 2018 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 HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity make 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 do 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.**