

One Identity Manager 7.1.5

Release Notes

March 2019

These release notes provide information about the One Identity Manager release, version 7.1.5. You will find all the modifications since One Identity Manager version 7.1.4 listed here.

One Identity Manager 7.1.5 is a patch release with enhanced features and functionality. See [Enhancements](#) on page 2.

If you update a One Identity Manager version that is older than One Identity Manager 7.1.4, read the release notes from the previous versions as well. You will find the release notes and the release notes about additional modules based on One Identity Manager technology under [One Identity Manager Support](#).

You will find a summary of the changes made in Web Designer since the last release in *Changes in Web Designer*.

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

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

About One Identity Manager 7.1.5

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

With this product, you can:

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

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

Enhancements

The following is a list of enhancements implemented in One Identity Manager 7.1.5.

Table 1: General known issues

Enhancement	Issue ID
The connection server already provided for transferring data to a One Identity Manager History Database is now used. To use this function, enable the configuration parameter HDB UseNamedLinkedServer in the One Identity Manager History Database and enter the connection server in the One Identity Manager History Database as server for the source database.	30028
Improved logging of error messages when transferring data to the One Identity Manager History Database.	30165
Improved performance when updating the One Identity Manager database.	30292
Improved logging in the application server.	30618
Improved performance in DBQueue Processor.	30763, 30626, 31293
The script VID_FindAndReplaceByLine has been deleted.	30632
Improved execution of templates through One Identity Manager Service.	30730
Improvements in the Job Queue Info.	31140

Enhancement	Issue ID
<ul style="list-style-type: none"> If the DBQueue contains more than 250000 calculation tasks, the operation There are more tasks to be processed is displayed in the DBQueue. This shows the number of queued tasks that cannot currently be shown in the DBQueue overview. 	
Process handling is interrupted during processing of DBQueue Processor triggers and constraints.	27486
Improved logging of terminated DBQueue slots.	30289
Improved protection of the application server's API.	31299, 31300
Improved protection against damaging SQL statements.	31299, 31301

Table 2: General web applications

Enhancement	Issue ID
Improved performance in the Web Portal for: <ul style="list-style-type: none"> Displaying the request history Editing questions about attestation cases Approving requests Determining an employee's entitlements 	30470, 30471, 30673, 30863, 31192

Table 3: Target system connection

Enhancement	Issue ID
Optimized calculation of inheritance for group memberships.	30076
Improved performance for individual provisioning of memberships and for synchronization.	30667, 30864, 30922
Improved performance synchronizing Microsoft Exchange recipient lists.	31163
Improved performance calculating Azure Active Directory group memberships.	30702
Property mapping rules that are no longer required are removed from the OwaMailboxPolicy map.	30498
A patch with the patch ID VPR#30498 is available for synchronization projects.	
Improved performance synchronizing Exchange Online recipient lists.	30959, 31162

Enhancement	Issue ID
In the Exchange Online connector, the list of error messages has been extended based on the assumption that the connection failed, by: An error caused a change in the current set of domain controllers. Your request is too frequent. Please wait for few minutes and retry. Topology Provider could not find the Microsoft Exchange Active Directory Topology service on end point.	31168
Spaces in distinguished names of LDAP objects are tolerated.	30542
Improved performance <ul style="list-style-type: none"> Calculating SAP functions Calculating SAP group, role and profile hierarchies. Synchronizing role assignments with the central system of a CUA (UserInCUARole) A patch with the patch ID VPR#30941 is available for synchronization projects.	30299, 30743, 30675, 30941

Table 4: Identity and Access Governance

Enhancement	Issue ID
If the option Temporarily disabled is not set for an employee and the date for Temporarily disabled from is in the future, the date for Temporarily disabled from and Temporarily disabled until are not deleted.	30344
Improved performance approving requests.	31341

See also:

- [Schema changes](#) on page 20
- [Patches for synchronization projects](#) on page 22

Fixes

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

Table 5: General

Resolved issue	Issue ID
Error testing email addresses for uniqueness, if an email address was	30300

Resolved issue	Issue ID
recalculated with a template but the old and the new values are identical.	
The function QBM_FSQRemoveComment does not recognize Linux carriage return.	30342
Ctrl+C does not copy the selected value in the Process step view in Job Queue Info.	30343
The script for selecting the server in a process step (Job.ServerDetectScript) is not implicitly extended by a Try-Catch-Block.	30347
If an object column and another column in the table QBMColumnTranslation are interrelated, the program exits because it cannot load these objects.	30380
Compilation fails if the process or process step contains quotation marks (") in names.	30403
Error filling raw tables if the One Identity Manager database and the History Database are installed in the same cluster.	30455
Under certain conditions, the database ends up in a trigger-free state if transport fails.	30459, 30447
Performance problems determining permissions.	30471
Wrong short name for the state of Newfoundland and Labrador .	30484
After extending the schema of custom read-only tables, new columns with the option Customer can configure are set to the value 0 .	30491
Error in the method SqlFormatter.NotInClause.	30505
Problems initializing the Job queue if a large number of queues are affected.	30539
The physical dependency between DBQueue Processor tasks does not consider tasks without parameters.	30573
Terminated slots are identified correctly if the SQL Server reuses the SPID.	30584
The procedures for shrinking the entries in the tables DialogWatchOperation, JobHistory and DialogProcessChain do not shrink in blocks.	30604
Timestamps on changes made in the database in Designer are shown in UTC.	30610
Triggers are not generated for DBQueue Processor tasks that record changes to configuration data.	30646
Migration does not remove non-linear dependencies correctly.	30693
In reports, IN clause queries on UID and XObjectKey columns are listed with Unicode strings.	30723
The limit for IN clause in report queries is not kept to correctly.	30724

Resolved issue	Issue ID
Error retrying process steps with the status MISSING .	30752
The procedure QBM_PCustomSQLFill fails with the message Violation of PRIMARY KEY constraint.	30753
There is a new consistency check Index name longer than 30 characters .	
The customizer method GetNextID fails when executed in Designer.	30786
Relaying processes is being blocked because the procedure QBM_PJobUpdateState is being called to frequently.	30798
If a Job destination ID contains a special character, the links on the One Identity Manager Service status page do not work.	30924
Job Queue Info ends unexpectedly, if there is a filter on the system journal and it returns a lot of entries.	30928
The procedure ProcessShrink leaves behind entries with BasisObjectType=<unknown Object> in the DialogProcess table.	31007
The state of Florida has the wrong timezone.	31089
Starting and ending the Database Compiler in Designer leaves a Wait for compiler entry in the DBQueue.	30094
The 's configuration data is always used when logging into a dynamic authentication module. Manager	30241
An error can occur during execution of DBQueue tasks in connection with the task QBM_PDBQueueReplGenProcID.	30272
Line breaks in the header of CSV files are not written back correctly. A CR is converted to a CR/LF .	30288
In certain circumstances, the procedure QBM_PIndexDropRedundant deletes required default indices.	30354
The One Identity Manager Service returns the process steps but the slots remain blocked.	31055
The procedure QBM_PDBQueueOverviewFill updated the table DBQueueOverview too frequently.	30800, 31217, 31296
Error in the German translation of entries in the DBQueueTasks table.	31117
Incorrect values in DialogCountry.NumericCode.	31352

Table 6: General web applications

Resolved issue	Issue ID
If a valid until date is specified for a request approval, the current time is used. The request is therefore not valid until the end of the given day.	30348
An employee can request membership in a specific business role.	30194
Incorrect where clauses are generated while index searching in many-to-many tables.	30679
Wrong display names for DialogSchedule.LastRun and DialogSchedule.NextRun in the Schedule Editor.	30687
Unsubscribed assignment requests are shown in the request history, although the option Canceled or denied or dismissed is not set.	30726
A request for a default service item New Active Directory security group cannot be approved.	30837
If an attestation request has been answered and saved, the dialog window remains open.	30845
Mandatory fields for attestation cases are not checked when queried.	30862
Although the option Display file content in browser whenever possible is set to False for downloading a file, the file content is still shown in the browser.	30404
Mapped functions in Web Designer are ignored if a parameter is defined.	30443
If a pending request is exported and an approval decision about this pending request is made, an error occurs.	30463
The Windows performance monitor does not show a value in the Web Portal performance indicator.	30699
In Chrome, you cannot browse through Hyper View pages in the Web Portal. Single shapes of a Hyper View can only be moved by clicking the header.	30790
If you edit a report subscription, the changes are not shown immediately in the report's detailed view.	30696
Some time data is only shown in English in the Web Portal.	31094
The filter settings for date columns are only available in English in the Web Portal.	31118
When a report is exported, the default template and not the custom template is used.	31231
In the Web Portal's configuration file (web.config), the URL /AE.axd is still declared.	31299, 31302

Resolved issue

Issue ID

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

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

In the section system.web\httpHandlers:

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

In the section system.webServer\httpHandlers:

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

Table 7: Target system connection

Resolved issue	Issue ID
Calculation of properties required for creating QueryByExamples objects does not recognize properties that are only loaded for matching by virtual ReadOnly properties.	30226
In Manager, changes to the value of IT operating data cannot be saved.	30295, 30746
Files in the synchronization user's temporary directory are not deleted.	30396
Error reading data from columns with data type varbinary if these are used as a primary key or part of one.	30474
Error loading synchronization projects.	30503
Provisioning tasks for group memberships are grouped under the wrong GenprocID.	30565
A maximum of 1024 modified memberships per group can be provisioned.	30597
Too many columns are loaded for resolving a reference.	30600
Running a clean up of the DPRMembershipAction table deletes entries that are still required.	30603
Synchronization deletes One Identity Manager database objects that are not unique in the target system.	30715
Processing of target system specific tasks in the DBQueue is blocked if this	30773

Resolved issue	Issue ID
target system is being synchronized at the same time.	
Objects that are added and provisioned in the One Identity Manager database while synchronization is running are duplicated in the database.	30957
Updating the schema or transporting a synchronization project removes the quota definition.	31098
The variable set loads too late when synchronization starts.	31152
The Active Directory connector returns empty elements for empty multi-value property columns.	29853
Incorrect handling of trusted domains in Active Directory synchronization projects. The project template has been corrected. A patch with the patch ID VPR#30192 is available for synchronization projects.	30192
Active Directory group memberships are not provisioned if the object SID for the user account is missing.	30509
Error processing unresolvable keys during Active Directory synchronization.	30552
Deleted values in the columns HomeDirectory and ProfilePath in Active Directory user accounts cannot be provisioned.	30561
Error calculating Active Directory group memberships if the user account's primary group has been changed.	30826
Error synchronizing the Active Directory user account schema properties ObjectKeyManager and Secretary. Synchronization quits although the option Continue on error is set.	30967
Timeout during synchronization of Azure Active Directory group memberships.	31051
If a Microsoft Exchange address list is marked as outstanding, the associated address book entries are not marked as outstanding.	30400
Error deleting outstanding Microsoft Exchange address book entries.	30401
If a Microsoft Exchange mailbox database is marked as outstanding, its server assignments are not marked as outstanding.	30466
Error provisioning deleted Microsoft Exchange mailboxes if deferred deletion is configured.	30807
Loading Microsoft Exchange data availability groups fails if all the servers involved are shut down.	31131
Error provisioning Exchange Online mailboxes. A patch with the patch ID VPR#31269 is available for synchronization projects.	31269

Resolved issue	Issue ID
The canonical name of LDAP objects are not formed automatically if the synchronization type is changed from No synchronization to One Identity Manager .	30398
Error setting up synchronization with IBM Notes if the connection to the Domino server is tested.	30427
Synchronization quits if the FullName of a Notes document cannot be loaded.	30691
The person document of a new Notes user account does not appear in the address book's default view.	30814
Error renaming a Notes user account if an organization unit is assigned to it.	30953
Flag Behavior inconsistent when handling SAPComPhone.PhoneType.	29725
The Synchronization Editor provides incorrect data for managers of organizational units from SAP HCM systems.	30121
Error loading SAP user accounts if the user account identifier contains quotes.	30258
When adding SAP user account with parameters, email addresses, telephone and fax numbers, distinguished names (such as SAPComPhone.DistinguishedName) are not formatted.	30356
Too many post-processing tasks are sent to the DBQueue if changes are made to SAP user accounts.	30361
The Insert event is not triggered for tasks in the HelperSAPUserInSAPRole table.	30367
SAP role assignments to SAP user accounts are provisioned, although the associated categories do not match.	30386
If several changes are made to an employee's central password in quick succession, by the Password Capture Agent for example, only the first change is made to the SAP user accounts.	30420
Company assignment of SAP user accounts is not provisioned in the target system. A patch with the patch ID VPR# 30453 is available for synchronization projects	30453
Error synchronizing company data (table Company).	30557
Error loading single objects for schema types that are provided by a schema extension file.	30653, 30701
Executable SAP transactions are not calculated correctly for SAP user accounts.	30718
Error calculating role assignments (table SAPUserInSAPRole).	30797, 31149

Resolved issue	Issue ID
Wrong templates for columns <code>SAPComPhone.PhoneNumber</code> and <code>SAPComFax.FaxNumber</code> .	31105
Error loading SAP user account if the name begins with a space character.	31329
During the calculation of SAP role assignments, those with <code>ValidFrom="1900-01-01"</code> and <code>ValidTo">"9999-12-31"</code> are ignored.	31361
Error converting Json data with the data type Integer or Float.	30536
Error deleting group memberships with the SCIM connector.	30710
Cloud application group memberships are incorrectly resolved if the schema property <code>members~type</code> does not contain a value.	31187
The connectors Microsoft Exchange, Exchange Online and Windows PowerShell only use one revision counter even if several schema properties per schema type are flagged as revision counters. In synchronization projects that use the Windows PowerShell Connector, the target system schema must be reloaded to use more revision counters. In synchronization projects for Microsoft Exchange and Exchange Online, a patch with the patch ID VPR#31026 is provided.	31026
An Out-Of-Memory exception occurs while determining managers for email users and email contacts in large Exchange Online systems.	31087
The native database connector does not delete group memberships in the target system if provisioning is carried out by an application server.	30659
During synchronization of the native database connector, objects are marked as changed although they have not been changed.	30840
In the process of adding a new Windows PowerShell connection, the consistency check does not notice if a schema class does not have a unique key.	31324
If changes are made to group properties, too many post-processing tasks are queued in the DBQueue.	30076
Post-processing tasks for outstanding objects that have been deferred, are not executed.	31180

Table 8: Identity and Access Governance

Resolved issue	Issue ID
Attestations are discontinued with the reason "No approver available" even though an approver is available.	30408
If an approval workflow is waiting for external approval and the approval step	30965

Resolved issue	Issue ID
EX is reached for a different attestation object, the external approval process is restarted for all pending objects.	
Under certain circumstances, the Customizer method CreateAttestations blocks DBQueue processing.	31016, 31370
Error deleting attestation cases.	31092
Disabling attestation policies does not delete the associated attestation cases.	31141
In email notifications to attestors, the pictures defined in custom mail templates are not shown.	31151
Service items cannot be added as products in the IT Shop if their identifier is longer than 128 characters.	30399
In the approval sequence, the time is shown as UTC time.	30483
Membership in a role cannot be delegated if the recipient of the delegation is already a member of this role.	30549, 30795
If a company resource is assigned by a limited period request and an unlimited period request at the same time and the limit period request expires, the company resource is removed although a valid, unlimited request still exists.	30697
The column templates ShoppingCartItem.ObjectKeyAssignment, DisplayObjectKeyAssignment and PersonWantsOrg.DisplayObjectKeyAssignment cannot be overwritten.	30766
Manager freezes when an approval workflow is copied.	30833
Initial login data is sent to the wrong employee when user accounts are requested in the IT Shop.	31014
Closed requests are not deleted, although the retention period must have expired.	31068
Incorrect testing of whether a company resource has already been assigned if the option Only for use in IT Shop is set.	31116
If an exception has been granted for a product with a rule violation in the approval process, the rule violation remains after the product has been canceled and the assignment removed.	30213
Ad-hoc rule checking does not create processing tasks for recalculating rule violations and for calculating the affected employee group. This means the affected employees may not be calculated correctly.	30281
If a disabled compliance rule is deleted, the associated rule violation is not deleted.	30585

Resolved issue	Issue ID
Calculating rule violations also calculates disabled rules.	30728
Error calculating compliance after updating the One Identity Manager database if only modules that are not dependent on the Compliance Rules Module are selected.	30905
The process CPL_PersonInNonCompliance_Assign_MitigatingControls is assigned to the wrong server function.	30994
Error assigning an object from a custom table to a system role.	30465
As from version 7.1.2, company resource assignments of child system roles are not mapped in the table EsetHasEntitlement. However, by updating the One Identity Manager database to version 7.1.2 or later, assignments to child system roles are not removed from the table EsetHasEntitlement.	30614
Missing risk indexes for system roles.	31337
In Manager, the Change security question task can also be displayed even though the logged in user does not have the required permissions.	30287
In the Show Entitlements Origin report, SAP roles and BI analysis authorizations that are inherited through system roles are missing.	30291

See also:

- [Schema changes](#) on page 20
- [Patches for synchronization projects](#) on page 22

Known issues

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

Table 9: General known issues

Known Issue	Issue ID
If you connect to a database with the Database Compiler, the task QBM-K-CommonWaitForCompiler is immediately queued in the DBQueue. If the Database Compiler ends without compiling the database, the task remains in the DBQueue.	23049, 24713
Error in the Report Editor if columns are used that are defined in the Report Editor as keywords.	23521

Known Issue**Issue ID**

Workaround: Create the data query as an SQL query and use aliases for the affected columns.

Error message in the Web Designer query window: Access to the path ... is denied. 23769

This error occurs if the user the web application process runs under, does not have write permissions for the given folder.

Errors may occur if the Web Installer is started in several instances at the same time. 24198

Header text in reports saved as CSV are not given their correct 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 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
```

Known Issue	Issue ID
<p>Number of parameter pairs ParamName/ParamValue in the MailComponent's process task SendRichMail is not always sufficient.</p> <p>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.</p>	25164
<p>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.</p> <p>Solution: Reload the object after completing simulation.</p>	12753
<p>Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation. This problem only occurs 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.</p>	25315
<p>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.</p>	27203
<p>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.</p> <p>Solution: Mark the private key as exportable if exporting or importing the certificate.</p>	27793
<p>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.</p>	28373
<p>The One Identity Manager Service only logs messages in the event log Application, by default.</p> <p>Cause: To add an event log with another name, you require administrator permissions on the Job server.</p> <p>Solution:</p> <ol style="list-style-type: none"> 1. Add the file that the One Identity Manager Service should write to manually on the Job server. You can use Windows PowerShell, for example, to do this. <ol style="list-style-type: none"> a. Run Windows PowerShell as administrator on the Job server. b. Run the following CmdLet: 	30540

Known Issue	Issue ID
<p>New-EventLog -Source "Foobar" -LogName "<file name>"</p> <ol style="list-style-type: none"> Enter this file name in the One Identity Manager Service's configuration file as the name for the event log in the module Logwriter . Restart the computer. Restart the One Identity Manager Service. 	
<p>The configuration parameter QER ITShop LimitOfNodeCheck specifies how many product nodes are deleted in one DBQueue Processor run if large numbers of products in the IT Shop are deleted through automatic processes. By default, 500 objects are processed in one run. Set the value lower if there are performance problems while executing the task QER-K-OrgAutoChild.</p>	30657
<p>Outstanding objects are ignored by inheritance calculation. This means, all memberships and assignments stay there until the outstanding objects have been processed.</p> <p>Run target system synchronization to do this.</p>	30909

Table 10: General web applications

Known Issue	Issue ID
<p>The error message This access control list is not in canonical form and therefore cannot be modified sometime occurs when installing the Web Portal with the Web Installer. The error occurs frequently after a Windows 10 Anniversary Update.</p> <p>Solution: Change the permissions for the users on the web application's parent folder (by default C:\inetpub\wwwroot) and apply the changes. Then revoke the changes again.</p>	26739
<p>Target system synchronization does not show any information in the Manager web application.</p> <p>Workaround: Use Manager to run the target system synchronization.</p>	30271
<p>It is not possible to log out of the Web Portal using OAuth 2.0/OpenID Connect because it is rerouted to a false address.</p> <p>Cause: If, in the configuration parameter QER Person OAuthAuthenticator LogoutEndpoint, a URL without a parameter is given, the logout parameters are appended to the URL in the configuration parameter in a format incompatible with the browser.</p> <p>Solution: Add a dummy parameter to the URL in the configuration parameter, for example, instead of http://localhost/IdentityManager/logout use the value http://localhost/IdentityManager/logout?from=logout.</p>	30999

Table 11: Target system connection

Known Issue	Issue ID
<p>Automatic employee assignment for Notes user accounts does not work.</p> <p>Cause: DialogObject.ObjectName on NDOUser has been renamed from NotesUser to NDOUser.</p> <p>Solution: Test the existing search criteria for employee assignment (table column NDODomain.AccountToPersonMatchingRule) and replace NotesUser with NDOUser.</p>	23270
<p>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.</p> <p>Example of an error message:</p> <p>[2134002] Error executing an adhoc projection!</p> <p>[1777239] The mapping rule (Members by SID) was unable to execute the projection between system objects (<group cn>) and (<group dn>) successfully!</p> <p>Solution: Delete the synchronization project and recreate it. Restore your customizations.</p>	24022
<p>Memory leaks occur with Windows PowerShell connections, which use Import-PSSession internally.</p> <p>After synchronizing an SAP R/3 environment, assignments of single role to SAP user accounts are labeled as outstanding.</p> <p>This problem can occur if:</p> <ul style="list-style-type: none">• SAP role assignments to user accounts were loaded in the One Identity Manager database before installing One Identity Manager 7.0.1• Single role assignments, which are included in collective roles, were mapped as direct assignments (Error ID 3218196) <p>By resolving this problem in One Identity Manager 7.0.1, incorrect assignments are labeled as outstanding after synchronizing again using the appropriate synchronization configuration.</p> <p>Solution: Delete outstanding assignments in One Identity Manager target system synchronization.</p>	23795
<p>By default, the building block HR_ENTRY_DATE of an SAP HCM system cannot be called remotely.</p> <p>Solution: Make it possible to access the building block HR_ENTRY_DATE remotely in your SAP HCM system. Create a mapping for the schema property EntryDate in the Synchronization Editor.</p>	25401

Known Issue	Issue ID
<p>Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses were stored up to now.</p>	27042
<p>The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3.</p> <p>If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration.</p> <ul style="list-style-type: none"> • Add a custom column to the table SAPUser. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required. 	27359
<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_UNKNOWNNNAME)).</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>	27687
<p>To use automatic employee assignment for central user administration (CUA) user accounts, assign an account definition to the CUA central system. Account definitions cannot be used to assign user accounts to child systems.</p>	28137
<p>If an Active Directory user account has the property MailNickName, an error occurs when the mailbox is enabled.</p> <pre>[System.Management.Automation.ActionPreferenceStopException] The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set to Stop: ExternalEmailAddress is mandatory on MailUser.</pre> <p>Cause: The property MailNickName is mapped in addition in the Active Directory mapping. This causes inconsistencies in the target system from the point the user accounts are added.</p> <p>A user account of this kind appears in the Microsoft Exchange console as a mail user but without a target email address. An attempt to open this object causes</p>	28820

Known Issue**Issue ID**

an object corrupted error in Microsoft Exchange.

Solution: Clear up inconsistencies in the affected user accounts in Active Directory and correct your Active Directory mapping.

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.

- 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 there are a large number of LDAP user accounts and LDAP groups in the database, provisioning might take a very long time. A message appears in the StdIO processor log(StdioProcessor.log) during the LDAP user account and LDAP groups update. 30172

```
DEBUG (SystemObjectData <static>) : Creating SystemObjectData based on entity (%DisplayName% (%cn%)) columns (UID_LDAPAccount, UID_LDAPContainer, UID_LDAPDomain, XObjectKey).
```

```
TRACE (SchemaElement static) : %DisplayName% (%cn%)@LDAPAccount[.GetValue (vrtScopeParentReference) returns ...
```

```
TRACE (SchemaElement static) : %DisplayName% (%cn%)@LDAPAccount[.GetValue (UID_LDAPContainer) returns ...
```

Cause: No reference scope is defined so that the default scope is used for resolving references. This causes too much data to be loaded from the database.

Solution: Define an empty reference scope. This means that scopes are not calculated when references are resolved, which noticeably improves performance with larger amounts of data.

Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled. 31017

Cause: The SharePoint connector loads all object properties into cache by default.

Solution:

- Correct the error in the target system.

Known Issue	Issue ID
<p>(missing or bad snippet)</p> <ul style="list-style-type: none"> Disable the cache in the file VI.Projector.SharePoint.<Version>.Host.exe.config. 	

Table 12: Third party contributions

Known Issue	Issue ID
<p>An error can occur during synchronization of SharePoint websites under SharePoint 2010. The method SPWeb.FirstUniqueRoleDefinitionWeb() triggers a ArgumentException. For more information, see https://support.microsoft.com/en-us/kb/2863929.</p>	24626
<p>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.</p>	24784
<p>Web applications under .Net 4.x on IIS are generally not stable if Microsoft Application Performance Monitoring is running on the same system. This problem is documented by Microsoft. For more information, see https://support.microsoft.com/en-us/help/3216459.</p>	28557
<p>Memberships in Active Directory groups of type Universal in a subdomain are not removed from the target system if one of the following Windows updates is installed:</p> <ul style="list-style-type: none"> Windows Server 2016 : KB4462928 Windows Server 2012 R2 : KB4462926, KB4462921 Windows Server 2008 R2 : KB4462926 <p>We do not know whether other Windows updates also cause this error. The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory groups during provisioning and will be removed in future once One Identity Manager has resolved the problem.Microsoft</p>	30575

Schema changes

No new changes to the schema have been made in One Identity Manager version 7.1.5 since version 7.1.4.

Synchronization template modifications

The following provides an overview of modified synchronization templates in One Identity Manager version 7.1.4. up to version 7.1.5. Apply the patches provided to the existing synchronization projects. For more information, see [Patches for synchronization projects](#) on page 22 and [Applying patches to synchronization projects](#) on page 44.

Table 13: Synchronization template modifications

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
Microsoft Exchange Module	Microsoft Exchange 2010 Synchronization	none
	Microsoft Exchange 2013/2016 Synchronization	none
Exchange Online Module	Exchange Online synchronization	changed
LDAP Module	AD LDS Synchronization	none
	OpenDJ Synchronization	none
IBM Notes Module	Lotus Domino synchronization	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	none
	SAP R/3 HCM employee objects	none
SharePoint Module	SharePoint synchronization	none
Universal Cloud Interface	SCIM Connect via One Identity	none

Module	Synchronization template	Type of modification
Module	Starling Connect	
	SCIM synchronization	none
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 7.1.5 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.

Table 14: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#30192	Scope definition and usage of processing method MarkAsOutstanding	Adds a scope and the processing method MarkAsOutstanding to the synchronization step trustedDomain.	30192

Table 15: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#30498	Removes property mapping rules from the OwaMailboxPolicy mapping	Removes property mapping rules BoxAttachmentsEnabled, DropboxAttachmentsEnabled and GoogleDriveAttachmentsEnabled from the OwaMailboxPolicy mapping.	30498
VPR#31269	Modified implementation by extending various property mapping rules by a condition.	In the Mailbox mapping, a condition was added to various property mapping rules to modify implementation.	31269

Table 16: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#30453	New property mapping rule for provisioning company data	New property mapping rule for mapping user account for provisioning company data.	30453
VPR#30941	Blacklist rule filter on "userInCUARole" step	Defines property mapping rules to be excluded from the provisioning workflow's process step userInCUARole.	30941

Patches in One Identity Manager version 7.1.4**Table 17: Patches for Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#29360	Prevents usage of employee mapping on insert	Marked employee mapping with Only suitable for updates.	29360
VPR#29410	Mapping of schema property ADSGroup.AllowWriteMembers	Inserts a property mapping rule for the schema property AllowWriteMembers in the group map.	29410
VPR#29837	Correct Active Directory site maps	Property mapping rule for object classes in the site mapping have been corrected.	29837

Table 18: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#30018	Connection parameters extended by an additional variable	Extends the target system connection parameters by an additional variable, PreferredServer.	30018

Table 19: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#29441	Corrects property mapping rules	Minor corrections of property mapping rules in Domain and Person mappings	29441

Table 20: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#29614	Corrected schema property vrtInactivePwd	Corrected the definition of the schema property vrtInactivePwd.	29614
VPR#29733	Apply revision filtering to user account communication data.	Applies revision filtering to the synchronization steps userComFax, userComPhone and userComSMTP.	29733
VPR#30160	Apply variable for SNC security settings to connection parameters	Applies the variable for SNC security settings to connection parameters. Depends on the patch New variable for SNC security settings (VPR#27420) that was provided with version 7.1.2.	30160

Table 21: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#30115	Corrected various properties in synchronization projects for personnel planning data.	Sets the option Data import in the synchronization steps Employee and OrgEH and corrects specific mapping properties in synchronization projects that were created with the project template for personnel planning.	30115

Table 22: 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.	29547

Table 23: Patches for the SCIM interface

Patch ID	Patch	Description	Issue ID
VPR#29454	Change to group mapping	Inserts a new property mapping rule for the group membership's type.	29454
VPR#30002	Correction of property mapping rules in the User mapping.	Corrected property mapping rules in User mapping in synchronization projects for One Identity Starling Connect applications.	30002

Patches in One Identity Manager version 7.1.3

Table 24: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#28560_ ADS	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
VPR#29299	Correction to Active Directory site handling	Corrected import of Active Directory sites and child machines.	29299
VPR#29318	Setting and removing maxPwdAge in domains	Corrects operation for resetting if maxPwdAge is set to never .	29318

Table 25: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#28560_ NDO	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560
VPR#28917	Revision counter changed.	Changed the revision counter. A new virtual schema property is used.	28917

Table 26: Patches for SAP R/3

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

Table 27: 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.	Corrected how to determine employees' SAP user account (USERID) and e-mail address (EMAILADDRESS)	28927

Table 28: Patches for the SCIM interface

Patch ID	Patch	Description	Issue ID
VPR#28560_SCIM	Display name conversion into English	German display names of property mapping rules and virtual schema properties are converted to English.	28560

Patches in One Identity Manager version 7.1.2**Table 29: Patches for Azure Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#27696	Prevents sync failure due to invalid license assignments	This prevents synchronization error on the bases of invalid dependency resolution of license assignments.	27496

Table 30: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#23447	Establish 2 rules for resolving trusted domain memberships	The patch changes the property mapping rule for group memberships. Some special features apply when you apply this patch. For more information, see the One Identity Manager 7.1.2 Release Notes	23447
VPR#27636	Remove extension property from ADSPolicy (in the One Identity Manager schema)	This patch removes the unnecessary schema property VRT_vrtADSPolicyAppliesToAsString from the schema class ADSPolicy.	27636

Table 31: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#28076	Add msRadiusFramedRoute mapping rule	Adds a property mapping rule for msRadiusFramedRoute in the mapping User.	28076
VPR#28106	Fixed Schemaclass Filter for MsImaging-PSPs	This patch corrects errors in the schema class filter for MsImaging-PSPs.	28106

Table 32: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#27379	Reconnect handling	This patch adds new connection parameters to restore disconnected connections. The variables CP_MaxConnectRetries and CP_ReconnectIntervalInSeconds can be defined in the synchronization project.	27379
VPR#27453	Configurable Active Directory settings	This patch adds new connection parameters for SetADServerSettings. The variables CP_ConfigurationDomainController, CP_PREFERREDGlobalCatalog and CP_SetPreferredDomainControllers can be defined in the synchronization project.	27453
VPR#27740	Prevents sync failure due to invalid public folder database master server references	This patch changes the virtual schema property vrtEX0Server of the schema class EX0PublicFolderDatabase to prevent synchronization error if the dependency cannot be resolved.	27740

Table 33: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#27801	Middle initial mapping	Mapping of schema property Middleinitial has changed.	27801
VPR#28123	Change group membership mapping	Changes the many-to-many schema type for user account memberships in groups of NDOUserInGroup (effective assignments).	28123

Table 34: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#12585	Create new rule on SAP user license to set license extension	Adds a property mapping rule in the mapping userHasLicense in synchronization projects for the central system of a CUA.	12585
VPR#27420	New variable for SNC security settings	Creates a connection variable for SNC security settings.	27420

Patch ID	Patch	Description	Issue ID
VPR#27588	Change to the column "Lock flag" mapping (SAPUser.U_Flag)	Behavior of locked user accounts in a central user administration has changed.	27588
VPR#27978	Changes the mapping rules of UID_SAPCompany field	Changes the property mapping rule for VRT_UID_SAPCompany to mapping user.	27978
VPR#28143	Change scope definition of SAP clients	Changes the scope definition for SAP clients in a central user administration (establish compatibility with Oracle Database).	28143

Table 35: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#27420	New variable for SNC security settings	Creates a connection variable for SNC security settings.	27420

Table 36: Patches for SAP R/3 BI analysis authorizations

Patch ID	Patch	Description	Issue ID
VPR#27420	New variable for SNC security settings	Creates a connection variable for SNC security settings.	27420
VPR#28141	Change user to BW role assignment behavior	Changes schema classes in the BWUserInBWProfile in One Identity Manager. Only assignments that are still in effect are taken into account.	28141

Table 37: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
VPR#26831	Apply new revision counters	Adds revision counters to the schema types SAPProfileHasAuthObjectElem, ObjectHasField and TMENU01.	26831
VPR#27420	New variable for SNC security settings	Creates a connection variable for SNC security settings.	27420

Table 38: Patches for the SCIM interface (Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#27627	OAuth2 grant type	Specifies the OAuth authentication access type.	27627

Patches in One Identity Manager version 7.1.1**Table 39: Patches for Azure Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902
VPR#27232	Change license assignment handling	This patch change the way license assignments are handled in One Identity Manager.	27232

Table 40: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902
VPR#26731	Reference scope correction	This patch corrects reference scope errors in forest trusts.	26731

Table 41: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#23842	Remove ObjectUSN from all mappings	Removes the property mapping rule for ObjectUSN from all mappings. Prerequisite for patch Marking member rules .	23842
VPR#26732	Reference scope correction	This patch corrects reference scope errors in forest trusts.	26732
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships. Dependent on the patch Remove ObjectUSN .	26902

Table 42: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902

Table 43: Patches for LDAP

Patch ID	Patch	Description	Issue ID
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902

Table 44: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#25351	Change state of variable "UserIDFilesDefaultPath"	The variable UserIDFilesDefaultPath can be changed after applying this patch.	25351
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902
VPR#27221	Adding an organizational unit	Adds an organizational unit to the employee mapping.	27221

Table 45: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#23478_1	Move SAP printer (part 1 of 2)	SAP printers moved from clients to the SAP system. Old property mapping rules deleted. Prerequisite for patch Move SAP printer (part 1 of 2) .	23478
VPR#23478_2	Move SAP printer (part 2 of 2)	SAP printers moved from clients to the SAP system. Add new property mapping rules. Dependent on patch Move SAP printers (part 1 of 2) .	23478
VPR#24597	Change phone data behavior	Flag Behavior changed when handling SAPComPhone.PhoneType.	24597
VPR#26902	Mark membership rules	This patch marks property	26902

Patch ID	Patch	Description	Issue ID
		mapping rules for editing memberships.	
VPR#27245	Change projection direction of some rules from 'inherit' to explicit direction	Changes the mapping direction of some property mapping rules to an explicit direction.	27245

Table 46: Patches for SharePoint

Patch ID	Patch	Description	Issue ID
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902

Table 47: Patches for the SCIM interface (Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#25214	Fill variables block	Inserts authentication variables into the default variable set.	25214
VPR#26497	Fill Resource Type Column	Inserts resource types for user accounts and groups.	26497
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902
VPR#26921	Lower reload threshold	Sets the reload threshold to 4 .	26921

Table 48: Patches for the Universal Cloud Interface interface (Cloud Systems Management Module)

Patch ID	Patch	Description	Issue ID
VPR#26666	Adjusts the synchronization configuration for pending changes.	Modifies the synchronization configuration for pending changes.	26666
VPR#26678	Corrects the account manager mapping	The Cloud group mapping is extended to the account manager.	26678
VPR#26854	One Identity Manager schema extensions	Extends the One Identity Manager schema.	26854
VPR#26994	Handling ineffective group	Ineffective group memberships	26994

Patch ID	Patch	Description	Issue ID
	memberships	are handled like deleted memberships.	

Table 49: Patches for Unix

Patch ID	Patch	Description	Issue ID
VPR#26902	Mark membership rules	This patch marks property mapping rules for editing memberships.	26902

Deprecated features

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

- Quick Connect Adapter
- PXE support
- Hardware inventory
- Software inventory
- Microsoft Exchange Server 2000 administration
- Microsoft Exchange Server 2003 administration
- Administration of printer locations to hardware
This function is replaced by direct administration of Active Directory printers.
- IT Shop voucher request using methods **Full Invoice** (FI) and **Invoice Item** (II)
- Archiving historical data using XML files (version 7.1.3 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 from 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**.

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

- Software distribution including
 - Driver admin
 - Application profile admin
 - Driver profile admin
 - PC Client
 - Profile Editor, Profile Scanner, Replication Info
 - Machine type admin
 - Structure for attended setup


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 2016• Windows Server 2012 R2

-
- Windows Server 2012
 - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
 - Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later

UNIX and Linux operating systems

- Note the minimum requirements given by the operating system manufacturer for Oracle databases.

Software

SQL Server

Following versions are supported:

- SQL Server 2016 Standard Edition, Service Pack 1 or later
- SQL Server 2014 Standard Edition, Service Pack 1 or later
- SQL Server 2012 Standard Edition, Service Pack 1 or later
- Compatibility level for databases: SQL Server 2012 (110)
- Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended)

i **NOTE:** The SQL Server Enterprise Edition is strongly recommended on performance grounds.

Oracle Database

Following versions are supported:

- Oracle Database 12c Standard Edition or Enterprise Edition Version 12.1.0.2 and later

i **NOTE:** Oracle Database version 12.2 or later is not supported.

- The patch level differs depending on the system platform.

i **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); parameter **NLS_LENGTH_**
SEMANTICSwith the 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 2016• Windows Server 2012 R2• Windows Server 2012• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later• Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later Linux operating system <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	Windows operating system <ul style="list-style-type: none">• Microsoft .NET Framework version 4.5.2 or later <p>i NOTE: Microsoft .NET Framework version 4.6.0 is not supported.</p> <p>i NOTE: Take the target system manufacturer's recommendations for connecting the target system into account.</p> Linux operating system <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	Windows operating system <ul style="list-style-type: none"> • Windows 10 (32-bit or 64-bit) with version 1511 or later • Windows 8.1 (32-bit or 64-bit) with the current service pack • Windows 8 (32-bit or 64-bit) with the current service pack • Windows 7 (32-bit or non-Itanium based 64-bit) with the current service pack • Windows Vista with the current service pack
Additional software	<ul style="list-style-type: none"> • Microsoft .NET Framework version 4.5.2 or later <p>i NOTE: Microsoft .NET Framework version 4.6.0 is not supported.</p>
Supported browsers	<ul style="list-style-type: none"> • Internet Explorer 10.0 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 <ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later • Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later Linux operating system

-
- Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.

Additional software Windows operating system

- Microsoft .NET Framework version 4.5.2 or later
 - **NOTE:** Microsoft .NET Framework version 4.6.0 is not supported.
- Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 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

- NTP - Client
- Mono 4.6 or later
- Apache HTTP Server 2.0 or 2.2 with the following modules:
 - mod_mono
 - rewrite
 - ssl (optional)

Minimum requirements for the Application Server

Processor 8 physical cores 2.5 GHz+

Memory 8 GB RAM

Hard 40 GB

drive
storage

Operating
system

Windows operating system

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later

Linux operating system

- Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.

Additional
software

Windows operating system

- Microsoft .NET Framework version 4.5.2 or later
 -  **NOTE:** Microsoft .NET Framework version 4.6.0 is not supported.
- Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 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

- NTP - Client
- Mono 4.6 or later
- Apache HTTP Server 2.0 or 2.2 with the following modules:

- mod_mono
- rewrite
- ssl (optional)

Supported data systems

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

Table 50: Supported data systems

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.
Connector for relational databases	Any relational databases supporting ADO.NET. i NOTE: Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer.
Generic LDAP connector	Any LDAP directory server conforming to version 3. The LDAP connector requires the directory server to be RFC conform. Specifically, to conform to the standards RFC 4514 (String Representation of Distinguished Names) and RFC 4512 (Directory Information Models). i NOTE: Other schema and provisioning process adjustments can be made depending on the schema.
Web service connector	Any SOAP web service providing wsdl. i NOTE: You can use the web service wizard to generate the configuration to write data to the web service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active Directory connector	Active Directory, shipped with Windows Server 2003 , Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2.
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

Connector Supported data systems

SharePoint connector	<ul style="list-style-type: none">• SharePoint 2010• SharePoint 2013
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	Supports the most common Unix and Linux derivatives. For more information, see the Authentication Services specifications.
IBM Notes connector	<ul style="list-style-type: none">• Lotus Domino Server Version 8.0 up to Lotus Domino Server Version 9.0• IBM Notes Client 8.5.3 is supported as client version.
Native database connector	<ul style="list-style-type: none">• SQL Server• Oracle Database• SQLite• MySQL• DB2 (LUW)• CData ADO.NET Provider• SAP HANA
Mainframe connector	<ul style="list-style-type: none">• RACF• IBM i• CA Top Secret• CA ACF2
Windows PowerShell connector	<ul style="list-style-type: none">• Windows PowerShell version 3 or later
Active Roles connector	<ul style="list-style-type: none">• Active Roles 6.9, 7.0
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.

Connector Supported data systems

Exchange Online connector

- Microsoft Exchange Online

Product licensing


This product does not require licensing.

Upgrade and installation instructions


To install One Identity Manager 7.1.5 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*.

Updating One Identity Manager to version 7.1.5

To update an existing One Identity Manager installation to version 7.1.5

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

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

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

- c. Click **Install**.

This starts the installation wizard.

- d. Follow the installation instructions.

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

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

6. Update the One Identity Manager Service on the server, which processes direct database queries.

- a. Execute the program autorun.exe from the root directory on the One Identity Manager installation medium.
- b. Change to the **Installation** tab. Select the Edition you have installed.

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

- c. Click **Install**.

This starts the installation wizard.

- d. Follow the installation instructions.

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

7. 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.
8. Start the One Identity Manager Service on the server, which processes direct database queries.
9. Update other installations on workstations and servers.

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

To update synchronization projects to version 7.1.5

1. 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 44.

To update an application server to version 7.1.5

- 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 7.1.5

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

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

To update the Manager web application to version 7.1.5

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

Applying patches to synchronization projects

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

Before you apply a patch

1. Read the patch description to decide whether it provides the necessary improvements for the synchronization project.
2. Check whether conflicts with customizations could occur.
3. Create a backup of the database so that you can restore the original state if necessary.
4. Deactivate the synchronization project.

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

To apply patches

1. Open the synchronization project in the Synchronization Editor.
2. Select **Edit | Update synchronization project...** from the menu.
3. In **Available patches**, select the patches you want to apply. Multi-select is possible. In **Details - Installation summary**, all patches are displayed in order of installation.
4. Click **Apply selected patches**.
5. Enter any user input as prompted.
6. Use the patch log to check whether customization need to be reworked.
7. If required, rework customizations in the synchronization configuration.
8. Run a consistency check.
9. Simulate the synchronization.
10. Activate the synchronization project.
11. Save the changes.

ℹ 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 21
- [Patches for synchronization projects](#) on page 22

Verifying successful installation

To determine if this version is installed

- Start the Designer or the Manager and select the menu item **Help | Info**.
You can see an overview of your system configuration on the **System information**.
The version number 2016.0010.0001.0500 for all modules and the application version 7.1 2016-10-01-319 indicate that this version is installed.

This patch updates all files that shipped with One Identity Manager 7.1.

Additional resources

Additional information is available from the following:

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

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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




Patents

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

Trademarks

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

Legend

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