

One Identity Manager 8.1.4

Release Notes

20 October 2020, 08:09

These release notes provide information about the One Identity Manager release, version 8.1.4. You will find all the modifications since One Identity Manager version 8.1.3 listed here.

One Identity Manager 8.1.4 is a patch release with new functionality and improved behavior. See [New features](#) on page 2 and [Enhancements](#) on page 3.

If you are updating a One Identity Manager version prior to One Identity Manager 8.1.3, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under [One Identity Manager Support](#).

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

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

You will find the current versions of the product documentation under [One Identity Manager Documentation](#).

About One Identity Manager 8.1.4

One Identity Manager simplifies the process of managing user identities, access permissions and security policies. It gives control over identity management and access decisions to your organization, freeing up the IT team to focus on their core competence.

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.

Starling Cloud Join

Initiate your subscription within your One Identity on-prem product and join your on-prem solutions to our One Identity Starling cloud platform. Giving your organization immediate access to a number of cloud-delivered microservices, which expand the capabilities of your One Identity on-prem solutions. We will continuously make available new products and features to our Starling Cloud platform. For a free trial of our One Identity Starling offerings and to get the latest product feature updates, visit cloud.oneidentity.com.

New features

New features in One Identity Manager 8.1.4:

Basic functionality

- New configuration option for detection and mail notification if the One Identity Manager Service stops processing queries.
Use the new **Common | MailNotification | NotifyAboutRequestStall** configuration parameter to specify whether to send a notification. The configuration parameter is not set by default. Use the new **Send notification when Job server is not requesting processes** schedule for the rest of the configuration. The schedule configuration must match the **Common | Jobservice | LoadedJobsTimeOut** configuration parameter.

Target system connection

- Support for One Identity Active Roles version 7.3.3, version 7.4.1, and version 7.4.3.

Identity and Access Governance

- Support for OAuth 2.0 authentication for Exchange Online mailboxes using attestation by mail and approval by mail.

The function uses the Exchange Web Service (EWS). Register an application in your Azure Active Directory tenant in the Microsoft Azure Management Portal. For example, **One Identity Manager Approval by Mail**. Enter the application ID that is generated by the registration in the new **QER | Attestation | MailApproval | AppId** and **QER | ITShop | MailApproval | AppId** configuration parameters.

For detailed information about how to register an application, see <https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth#register-your-application>.

See also:

- [Enhancements](#) on page 3
- [Resolved issues](#) on page 5
- [Schema changes](#) on page 25
- [Patches for synchronization projects](#) on page 27

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.1.4.

Table 1: General

Enhancement	Issue ID
Extended the scope of SQL logging if SQL queries need to be repeated.	33268
Exceptions that caused the SQL query retries are logged.	33462
Improved testing of multiple name properties in password policies if the Name properties denied option is set.	33245
Improved performance for various SQL functions.	33066, 33080
Improved performance transferring to the History Database.	33438, 33439
Reduced processing time in the DBQueue due to optimized setting of automatically generated calculation tasks.	33454
Optimized internal database communication to coordinate processing of DBQueue Processor tasks. The volume of internal database messages	33453

Enhancement	Issue ID
(MessageBroker) has been reduced. In addition, using the same sort order, post-processing tasks with less succeeding tasks are prioritized over those with a lot of succeeding tasks to reduce the total number of tasks pending at the same time.	

Table 2: General web applications

Enhancement	Issue ID
Improved performance determining the service items used for requests in the Web Portal.	33256
In the Web Portal, empty date fields are now shown with an example value so that you can quickly identify the expected date format.	33493
The following JavaScript libraries have been updated: <ul style="list-style-type: none"> • Bootstrap: Version 3.4.1 • AngularJS: Version 1.7.9 	254323

Table 3: Target system connection

Enhancement	Issue ID
In the Manager, the general data form for target system types shows the AdditionalSystemTypes (Alternative connectors) column.	33366
The SCIM connector supports SCIM provider cookies in REST queries.	33051
The SAP connector supports setting of current passwords for login using Secure Network Communications (SNC) with Single Sign-On.	33455, 33461
Corrected SAP companies reference to SAP user account for SAP S/4HANA 2.0 support. A patch with the patch ID VPR#32347 is available for synchronization projects.	32347
Improved display of test results if the SCIM endpoint connection is tested in the system connection wizard for cloud applications.	33232
Improved logging of native database connectors when establishing a database connection using the generic ADO.NET provider.	33079

See also:

- [Schema changes](#) on page 25
- [Patches for synchronization projects](#) on page 27

Resolved issues

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

Table 4: General

Resolved issue	Issue ID
<p>Administrative users are missing permissions that allow information to be found in the <code>dbo.sysjobhistory</code> table about running database schedules through the SQL Server Agent.</p> <p>To grant the permissions, run the following SQL statement in a suitable program.</p> <pre>use msdb go GRANT SELECT ON OBJECT::sysjobhistory TO [OneIMRole_<DatabaseName>] go</pre>	33179
<p>Although the database is not encrypted, the encrypted option can be enabled for custom configuration parameters.</p>	33089
<p>When copying permissions groups, an error occurs in the copy wizard: Copy started. Copy failed with following error: [810025] DialogColumnGroupRight: Write permission denied for value "CanEdit".</p>	33253
<p>The QBMRelation invalid (QBM_FTRelationValidationInfo) consistency check is considered invalid if there is a table relation, added by Schema Extension, of a database view, type View, (for example Department to a table of type Base table (for example Basetree).</p>	33130
<p>If the Skript (OnDiscarded) table script is completely empty, the Skript (OnDiscarding) table script does not run. The problem does not occur if there is something in the Skript (OnDiscarded) table script, a comment for example.</p>	33252
<p>A subscribed report with the Simple list report option does not contain a header.</p> <p>From One Identity Manager version 8.0 onward, simple list reports are not created by the Export process task of the ReportComponent but by the CSVExportSingle process task of the ScriptComponent process component. During the conversion, the headers (parameter Header) were forgotten.</p> <p>The RPS_ParseReportDefinitionXML script was amended. The RPS_RPSSubscription_Send_Report, RPS_RPSSubscriptionCC_Send_Report_to_CC, RPS_RPSSubscription_Store_Report, and RPS_RPSSubscriptionCC_Store_Report_for_CC processes were modified.</p>	33261

Resolved issue	Issue ID
<p>Maintenance tasks for rebuilding the table index (QBM-K-CommonReIndexTable) take a long time to run or fail due to the length of runtime, are retried and, therefore, never vanish from the DBQueue.</p> <p>: The statistics update has been removed from the QBM-K-CommonReIndexTable task and stored in a new task called QBM-K-UpdateStatistics. The task does not update the statistics for each table individually but runs the stored procedure sp_updatestats. This improves the update's performance.</p>	33172
<p>Running changes in parallel that were added to the DialogProcess table, potentially causes the error: VI.DB.DatabaseException: Database error 2627: Violation of PRIMARY KEY constraint 'PK__DialogPr__2B66FD776487EDFB'. Cannot insert duplicate key in object 'dbo.DialogProcess'.</p>	33188
<p>In version 8.1.x, it is not possible to log in to the Launchpad with the Active Directory user account (role-based) and Active Directory user account (manual input/role-based) authentication modules.</p>	33318
<p>It is possible that a huge number of tasks for recalculating the approver (QER-K-ShoppingRackPWOHelperPWO-Cfg) occur in the DBQueue thus blocking other tasks.</p>	33083
<p>In the Schema Editor, the ViewAddons tab disappears sporadically. You have to click back and forth in order to show the tab.</p>	33171
<p>Tasks that persist for a long time in the DBQueue and are repeated again and again, disappear eventually from the DBQueue without being calculated.</p>	33338
<p>An error occurs when granulated permissions are issued for objects that do not belong to the dbo schema: Cannot find the object 'MyTable', because it does not exist or you do not have permission.</p> <p>Objects are now tested to check that they belong to the dbo schema when granulated permissions are issued. Objects foreign to the schema are not issued granulated permissions.</p>	33164
<p>An error occurs during installation of the History Database in a managed instance in the Azure SQL Database: Database error 41906: Statement ',BEGIN DISTRIBUTED TRANSACTION' is not supported in SQL Database Managed Instance.</p>	33307
<p>Relatively small values in the Common ProcessState PackageSizeHDB configuration parameter are not taken into account when data is transferred to the History Database.</p>	33363
<p>The Service account and Read-only options can be enabled at the same time for system users.</p> <p>The behavior has been changed. The options cannot be enabled together anymore.</p>	33195

Resolved issue	Issue ID
Error creating a custom form with the VI_Common_Assignment_Overview (FrmCommonAssignmentOverview) form definition.	33325
In the dialog for an object's extended properties, the Permissions tab does not display the edit properties for the permissions groups correctly.	33464
Errors can occur on saving additional view definitions (QBViewAddOn) if so much data has already been saved in the view definition in the database so that the data is stored externally in the SQL Server (Blob (extern) is set).	33409
If slots for the DBQueue Processor are being loaded because, according to the QBM DBQueue KeepAlive configuration parameter, the maximum lifetime has been reached, the number of messages of the following type written to the system log might increase: #LDS#Dead slot resetted, number={0}, type = {1}, Task = {2}, code = {3}. 4 DeadTest <none> 2	33460
The Tree level (TreeLevel1) column in views derived from the BaseTree table, are not populated when new objects are added. For example, application roles.	33489
Reports with historical data show inactive assignments as still being assigned. In the report, the Assigned until column is empty.	33393

Table 5: General web applications

Resolved issue	Issue ID
In certain circumstances in the Web Portal, an error occurs opening large reports.	32896
In the Web Portal, the text for justifying an approval about a pending request is populated with the text of a previous, completed approval.	33152
Logging in to the Password Reset Portal using the link in the login email does not work.	32885
Incorrect translation in the DialogMultiLanguage table causes an error when the password policy is used in the Password Reset Portal.	33278
The following error occurs while compiling a web project: An error occurred while generating source code in <web project>. Error while generating code for configuration key: TableSearch_Person Object reference not set to an instance of an object.	33346
In the Web Portal, links in an object's details pane do not work.	33210
In certain circumstances, an error occurs updating the preview in the Web Designer.	33180

Resolved issue	Issue ID
In the Web Portal, the Delete all my delegations button on the Delegations page only deletes the first page of delegations.	33186
In the Web Portal, group memberships that are indirectly assigned through child groups are not shown anymore.	33216
In the Web Portal, if the approver of an attestation case does not grant approval and this leads to a product being unsubscribed, the recipient is shown incorrectly as the approver in the corresponding request's history.	33255
In the Web Designer, you can set validity dates for all the products in a shopping cart. Products that already have a validity date or period are not taken into account in this case.	33322
In the Web Portal, when you edit the shopping cart, the Replace already specified dates box option is now available for both Valid from and Valid until . You can apply this option to all the products in the shopping cart regardless of the dates set individually on a product.	
In the Web Portal, when a product is being renewed, it is possible to extend the validity of a product beyond its permitted limit.	33410
In the Web Portal, an error occurs if a request approver initially sets the wrong expiry date but then corrects it.	33343
In certain circumstances in the Web Portal, new subscriptions are incorrectly deleted during editing.	33468
Tabs on the monitor page of the Web Portal do not contain any information.	33457
In certain circumstances, the search in the Web Portal does not find the search object.	33387
In certain circumstances, the application server quits unexpectedly when an indexing instance is started.	33174
When charts are displayed in the Web Portal, an error if all those to be displayed are deselected using the chart filter.	33501
An error occurs while compiling the API Designer if a relative path is used in the .config file.	33505
If the Web Portal is connected directly to the database, there are heavy delays and long load times.	33470
If you open the <WebPortal>/ae.axd page to test the connection to the Web Portal, a new session is set up.	33389
An error occurs if you request a product in the Web Portal and the request is subsequently canceled through the request history.	33146

Table 6: Target system connection

Resolved issue	Issue ID
Memberships that have been added to One Identity Manager but not yet provisioned are marked as pending by a synchronization running at the same time.	33144
When using the Database Transporter to import a synchronization project, the Do not change the start up configuration settings import option is not taken into account if it is enabled. Changes to the start configuration and to variables are overwritten in the target database.	33153
If a membership is added to the One Identity Manager that has been previously deleted during target system synchronization, the change is not provisioned in the target system.	33201
Under certain circumstances, when provisioning object properties, memberships of the affected objects in the target system are completely replaced with the memberships that exist in One Identity Manager, even though single provisioning of memberships is configured. This leads to changes made directly in the target system being overwritten. The error occurs when schema properties dependent on an M:N property are to be provisioned. Due to the dependency, the memberships are also provisioned. If there is no membership operation in the DPRMembershipAction table at this time, the complete membership list is transferred.	33205
If script variables are used in a variable set, the values of the default variable set are written to the synchronization log for the script variables instead of the values of the used variable set. During synchronization, the correct variable values are used. Only the logging of the script variables is incorrect. Only logging of the script variables is incorrect.	33229
Under the following conditions, the transport package for a synchronization project cannot be imported: <ul style="list-style-type: none"> • The synchronization project already exists in the target database. • The source project does not contain all the objects referenced in the target project. This causes an FK violation.	33257
When transporting synchronization projects, the table relations' Ignore in superset handling property is not taken into account. The Database Transporter tries to delete referenced objects that exist in the target database but are missing in the transport package.	
Error provisioning new memberships that have been deleted again in the One Identity Manager database (xOrigin='0') before the provisioning process for	33267

Resolved issue	Issue ID
the new additions has been completed.	
If single provisioning of memberships is configured for different custom target system types, several entries in the DPRMemberShipAction table are generated each time a membership is changed. One entry is created per target system type for which merge mode is set in the UNSAccountBInUNSGroupB table. However, only one entry is expected for the target system type containing the modified membership.	33365
In the Synchronization Editor, if maintenance of synchronization buffers is started manually, an error message appears, which says that the DPR_MaintainDataStore process cannot be generated.	33391
Error opening a synchronization project in the Synchronization Editor with a user that only has read permissions: Write permission denied for values: EditedBy, EditedSince.	33394
When the Synchronization Editor opens a synchronization project, it writes the current user and time to the project and saves it in the One Identity Manager database (DRPShell table). This function prevents loss of data by informing other users, who try to open the same synchronization project, that it is already in use. However, the Synchronization Editor does not check if the current user has write permissions for this table.	
In the synchronization log, an object is logged as modified. However, no change is logged for an object property although the synchronization log is configured such that modified properties and values are logged.	33402
If the modified object property contains a secret value or the NULL , this change is not written to the synchronization log.	
Solution: Logging has been altered. Secret values are logged as <hidden> and NULL values are logged as <null> .	
Property mapping rules with a restricted direction of mapping and the addition Ignore mapping direction restraint on insert , do not work if synchronizing in the direction of the target system.	33437
Certain Objects cannot be loaded during synchronization with a native database system. The following error message appears: No suitable key property found for reloading!	33258
The value of the key property corresponds to the default value of the respective data type. For example, if the primary key has the Integer data type and a value of 0 , the native database connector interprets it as empty and does not use the value to select the object.	
SQL error synchronizing with the native database connector if, in the connection configuration to the external database, a pattern-based strategy for running data operations is defined and a referenced column name contains	33274

Resolved issue	Issue ID
<p>a space character.</p> <p>Solution: The database connector uses the <code>ScriptSafeIdentifier</code>. Column names with special characters are now referenced if the special character is replaced by an underscore. Special characters are everything apart from letters, numbers and underscore.</p> <p>Example: <code>Insert Into MyTab([ColPK],[Col Spaces]) Values(%ColPK%, %Col_Spaces%)</code></p>	
<p>New objects cannot be loaded during synchronization with a native database system. This error message appears: Unable to create the primary key where clause for system object ...</p>	33370
<p>Error setting up a synchronization project for a CData ADO.NET Provider database with the native database connector. The error only occurs if the driver version 2020 is used.</p>	33484
<p>The synchronization templates for Oracle E-Business Suite and SCIM add the reference scope with a German display name.</p> <p>Patches with patch IDs VPR#33259_SCIM and VPR#33259_EBS are available for synchronization projects.</p>	33259
<p>Error writing objects with the SCIM connector if the target system does not support queries with the Expect: 100-continue HTTP header option. The query is answered with HTTP status 417 Exception failed. The SCIM connector identifies this as an error and ends the process.</p>	33220
<p>If a complex schema property is defined in the SCIM connector schema, its child schema properties might not be returned by the SCIM connector. Thus the schema properties are missing in the Synchronization Editor. For example, in the target system's schema view in the MappingEditor.</p>	33233
<p>If a complex schema property is marked as a mandatory property in the SCIM schema, provisioning fails because a mandatory property is not mapped.</p>	33241
<p>Error synchronizing with the SCIM connector if the <code>id</code> schema property of an object is a compulsory field.</p> <p>In One Identity Manager, the <code>id</code> schema property is labeled as read-only in adherence with the SCIM specification. If the custom schema extension of the <code>id</code> schema property is added to an object as writable, the property is still mapped as read-only in the One Identity Manager's extended schema. Therefore, in the object's PUT request, the <code>id</code> is not transferred. The SCIM provider responds with the error <code>Missing required attribute [id]</code>.</p>	33336
<p>Error provisioning memberships if the SCIM provider supports the PATCH method.</p> <p>An error occurs in SCIM when writing the <code>members~vrtIDandType</code> virtual schema</p>	33459

Resolved issue	Issue ID
property, which should distribute individual values to the <code>members~type</code> and <code>members~value</code> child schema properties.	
The SCIM connector does not properly state that a SCIM provider does not supports filters. System filters can be defined in the synchronization project. However, this is not effective if the SCIM connector accesses the target system.	33483
In One Identity Manager you can create Active Directory objects that differ only in diacritical characters (for example ê, ü). This is not permitted in Active Directory. A process step with the status Frozen is created because this object already exists in the Active Directory.	33032
The home and profile directory of an Active Directory user account are deleted immediately once the user account is marked for deletion.	33202, 33092
In Manager, if you open the master data form for several Active Directory groups selected by multi-select and open the Account manager drop-down menu on the form, then the program no longer reacts.	33177
If an Active Directory schema in an existing synchronization project is updated after it was created by a project template, all the schema types that were not already saved in the schema are missing the contents from the calculated schema properties <code>AuxiliaryClasses</code> , <code>ContainerClasses</code> , <code>AllSuperClasses</code> , and <code>AllSearchClasses</code> .	33246
Assigning an Active Directory computer to a device does not queue a <code>ADS-K-ADSMachineInADSGroup</code> recalculation task. This means that groups inherited through the device are not assigned to the computer.	33420
On the master data form for Active Directory user accounts, the control for the Dial-up permitted property is always enabled, even if the user only has read-only access to the property. The value can be changed and saving does not cause an error. However, the changes are not saved.	33463
The type testing for loading Active Directory object is too strict.	33138
Error assigning an employee to an Active Directory user account if the user account has a linked Microsoft Exchange mailbox without being linked to a user account (<code>EX0Mailbox.UID_ADSAccountLinkedMaster</code>).	33317
The contact data of an Azure Active Directory user account with an Exchange Online mailbox can only be maintained if the mailbox is of recipient type User Mailbox (<code>UserMailbox</code>).	33191
Error synchronizing Azure Active Directory groups that are assigned to Azure Active Directory administrator roles.	33399
To correct this issue, a member filter that only includes user accounts has been defined in the DirectoryRole mapping. A patch with the patch ID	

Resolved issue	Issue ID
VPR#33399 is available for synchronization projects.	
Exchange Online synchronization fails when updating telephone numbers of Exchange Online mail users linked to an Azure Active Directory user account of type Guest .	33476
A patch with the patch ID VPR#33476 is available for synchronization projects.	
The columns O3EDynDL.Notes, O3EMailContact.Notes, O3EMailUser.Notes, and O3EUnifiedGroup.Notes are too short.	33392
Error message insufficient when parsing the distinguished name (DistinguishedName) of an LDAP object. The failed object does not appear in the message.	33310
Error loading SAP user accounts if SAP client salutations are defined that are identical in more than one language. The salutation references cannot be resolved.	33147, 33447
A patch with the patch ID VPR#33147 is available for synchronization projects.	
In the Synchronization Editor, if you open the target system browser for a connected SAP R/3 environment and select a single object in any result list, no object properties are displayed.	33168
When extending the SAP schema with a schema extension file, no error is detected if the OutStructure attribute in a function definition has the correct data type BAPIRET2, but the name of the SAP structure is not RETURN, RETURNØ or BAPIRET2.	33200
If different tables are used in the schema type definition of a schema extension file for calling the object list or calling single objects, SAP R/3 only accesses the tables with the ListObjectsDefinition attribute when setting up the schema and loading objects.	33218
SAP roles are labeled as deleted or outstanding by synchronization if the same role is inherited both as single role and through a collective role as well. This happens when the TargetSystem SAPR3 KeepRedundantProfiles is set.	33244
The overview form for an SAP role does not show which IT Shop shelves the role is assigned to.	33361
During synchronization with an SAP R/3 environment, the error messages in the synchronization log multiply if Continue on error is set in the synchronization project.	33416
If a change to the salutation in an SAP user account is provisioned, the Check Properties SAP check fails. This happens if the SAP R/3 connector accesses the target system during provisioning using a login language other than the	33423

Resolved issue	Issue ID
original language of the salutation. A patch with the patch ID VPR#33423 is available for synchronization projects.	
If an employee's central password is changed in One Identity Manager, this employee's SAP user account is locked.	33450
If a connection to IBM Notes cannot be established immediately because another process is already using the system, the connection waits for the process to end and a warning is issued if it cannot connect while waiting. To issue the warning, access is required to a property of a Domino Server that cannot be reached. The follow error occurs: "Domino server not connected."	33283
If the TargetSystem NDO MailBoxAnonymPre configuration parameter is not set, Notes user accounts are not anonymous when they are locked. If these user accounts are later unlocked, the NDO_NDOUserInGroup_ChangeNamesOn (un)Lock process is run although the full names of the user accounts have not been changed.	33330

Table 7: Identity and Access Governance

Resolved issue	Issue ID
Under certain circumstances, the QER_Person_Publish_CentralPassword process runs several times in parallel for the same object. This may happen if passwords have been changed several times within a One Identity Manager Service processing interval for this Job server. In this case, several of these processes are in the queue at the same time and are processed simultaneously. To enforce the correct processing order, the QER_Person_Publish_CentralPassword process step in the Publish password to all accounts process has been changed from the ScriptExec process function to the ScriptExecExclusive process function.	33132
Error calculating the attestor in the ATT_PAttestationHelperFill procedure. Although no regular attestor can be found for a decision step, the attestation case is not transferred to the fallback approvers. The decision step is automatically denied. This happens if the QER Attestation PersonToAttestNoDecide configuration parameter is set and the employee being attested is found to be the only attestor.	33151
Incorrect approvers are determined by the Attestation of assignments to system entitlements (including Active Directory) approval workflow. Target system managers are determined for Active Directory groups and product owners for all other system entitlements. However, it should be the other way round.	33187

Resolved issue	Issue ID
<p>During calculated approval, the reason text defined in the approval step (Approval reason or Reject reason) is not entered in the attestation case. Instead, the standard reason text of "Automatic system approval with method CD..." is used.</p> <p>The ATT_ZAttestationMakeDecisionCD SQL procedure has been corrected.</p>	33344
<p>If attestation cases for permanently disabled employees are automatically closed, the reason for the approval decision remains unchanged. Therefore, you do not know the reason why it was closed.</p> <p>The ATT_TUPerson trigger was changed. Closed attestation cases now have the following reason text: "Automatic system approval: Case closed due to employee becoming inactive."</p>	33345
<p>In the case of an approval step, if there is more than one entry for the same employee in the AttestationHelper table, let us say, as an attestor and as a chief approval team, it is possible, during delegation of an approval, that a member of the chief approval team delegates their responsibility and the employee can still make approvals as a regular attestor of attestation cases.</p>	33360
<p>Deadlocks can occur if entries are deleted in the auxiliary table for request procedures (PW0HelpPW0 table) after an approval procedure is complete. Deletion tasks are queued in both in the Job queue and in the DBQueue for the same closed request. These conflict.</p>	33327
<p>The Azure Active Directory > Basic configuration data > Target system type menu item (AzureAD.BasicInformation.DPRNameSpace) does not show the Exchange Online target system type.</p>	33368
<p>The ATT-K-AttestationHelper-Cfg task reoccurs far too frequently in the DBQueue. This effect is further amplified by migrating to One Identity Manager 8.1.2. This causes a heavy load on the DBQueue, which means that other tasks are not processed promptly.</p> <p>By changing employee assignments and updating One Identity Manager, the QER-K-AllForPersonInBaseTree task is queued per employee in the DBQueue. This leads to a recalculation of the ATT-K-AttestationHelper-Cfg task for each employee and queues this task for every pending attestation case.</p> <p>The ATT_PAttestationHelperFillAll and QBM_ZRecalculate procedures are modified such that ATT-K-AttestationHelper-Cfg tasks are not queued more than once in the DBQueue for the same attestation case.</p>	33082
<p>Sometimes assigned requests are canceled after the product is moved to another shop although the employee is still a customer in the new shop.</p>	33137
<p>If the timeout is exceeded, approval steps are not automatically approved as long as the timeout is still valid for a member of the chief approval team.</p>	33436

Resolved issue	Issue ID
If the employee has a lot of watch operations, the front-end (for example, the Manager or the Report Editor) unexpectedly quits when the Overview with business roles and user accounts (incl. history) report opens.	33502

Table 8: IT Service Management

Resolved issue	Issue ID
If the QBM WorkingHours IgnoreWeekend configuration parameter is set, the default working hours from countries and states are not taken into account.	33414

See also:

- [Schema changes](#) on page 25
- [Patches for synchronization projects](#) on page 27

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
Error in the Report Editor if columns are used that are defined in the Report Editor as keywords. Workaround: Create the data query as an SQL query and use aliases for the affected columns.	23521
Errors may occur if the Web Installer is started in several instances at the same time.	24198
Header text in reports saved as CSV are not given their correct names.	24657
In certain circumstances, objects can be in an inconsistent state after simulation in Manager. If an object is changed or saved during simulation and the simulation is finished, the object remains in the final simulated state. It may not be possible to save other modifications to this object instance. Solution: Reload the object after completing simulation.	12753

Known Issue	Issue ID
<p>Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation.</p> <p>Cause: The Configuration Wizard was started directly.</p> <p>Solution: 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 or the API Server if the certificate's private key, used by the VI.DB to try and encrypt its session data, cannot be exported and the private key is therefore not available to the VI.DB.</p> <p>Solution: Mark the private key as exportable if exporting or importing the certificate.</p>	27793
<p>It is not possible to extend predefined dynamic foreign keys by references to redefined tables. If you define custom dynamic foreign keys, at least one of the parties involved - dynamic foreign key column or referenced table - must be a custom object.</p>	29227
<p>Error resolving events on a view that does not have a UID column as a primary key.</p> <p>Primary keys for objects in One Identity Manager always consist of one, or in the case of M:N tables, two UID columns. This is basic functionality in the system.</p> <p>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.</p> <p>The consistency check Table of type U or R with wrong PK definition is provided for testing the schema.</p>	29535
<p>The default setting of globallog.config assumes that write access exists for %localappdata%. If an EXE does not have sufficient permissions, the log can be written to a directory that does have the access rights by changing the variable logBaseDir in the globallog.config or by introducing a special log configuration in the *.exe.config or the Web.config file.</p>	30048
<p>If the One Identity Manager database is installed in an SQL cluster (High Availability Group) and the option DTC_SUPPORT = PER_DB is set, replication between the server is done by Distributed Transaction. The error, in case a Save Transaction is carried out is: Cannot use SAVE TRANSACTION within a distributed transaction.</p> <p>Solution: Disable the option DTC_SUPPORT = PER_DB.</p>	30972
<p>If no date is given, the date 12/30/1899 is used internally. Take this into</p>	31322

Known Issue	Issue ID
account when values are compared, for example, when used in reports. For detailed information about displaying dates and time, see the <i>One Identity Manager Configuration Guide</i> .	
The following error occurred installing the database under SQL Server 2019: QBM_PDBQueueProcess_Main unlimited is only allowed as an agent job Solution: <ul style="list-style-type: none"> The cumulative update 2 for SQL Server 2019 is not supported. For more information, see https://support.oneidentity.com/KB/315001 .	32814

Table 10: Web applications

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 the web application's parent folder (by default C:\inetpub\wwwroot) and apply the changes. Then revoke the changes again.	26739
In the Web Portal, a product's request properties are not transferred from the original request to the shopping cart if the request is renewed or canceled. Cause: Request properties are saved in separate custom columns. Solution: Create a template for (custom) columns in the ShoppingCartItem table that stores the request properties when the request is made. This template must load the request properties from the identical (custom) columns in the PersonWantsOrg table relating to this request.	32364
It is not possible to use the Web Designer to place a link in the header of the Web Portal next to the company name/logo.	32830
In the Web Portal, it is possible to subscribe to a report without selecting a schedule. Workaround: <ul style="list-style-type: none"> Create an extension to the respective form that displays a text message under the menu explaining the problem. Add a default schedule to the subscribable report. In the Web Designer, change the Filter for subscribable reports configuration key (VI_Reporting_Subscription_Filter-RPSSubscription) and set the schedule's Minimum character count value (UID_DialogSchedule) to 1. 	32938

Table 11: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use Import-PSSession internally.	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
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.	27042
<p>Error in IBM Notes connector (Error getting revision of schema type ((Server))).</p> <p>Probable cause: The IBM Notes environment was rebuilt or numerous entries have been made in the Domino Directory.</p> <p>Solution: Update the Domino Directory indexes manually in the IBM Notes environment.</p>	27126
<p>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>Synchronization projects for SAP R/3 that were imported by a transport into a One Identity Manager database, cannot be opened. The problem only occurs if an SAP R/3 synchronization project was not added in the target database before importing the transport package.</p> <p>Solution: Create and save at least one SAP R/3 synchronization project before you import SAP R/3 synchronization projects into this database with the Database Transporter.</p>	27687
<p>Error 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>	29253

Known Issue	Issue ID
<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. 	
<p>Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will not come into effect until later.</p>	29556
<p>Cause: The function BAPI_EMPLOYEE_GETDATA is always executed with the current date. Therefore, changes are taken into account on a the exact day.</p>	
<p>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.</p>	
<p>Error synchronizing an OpenDJ system, if a password begins with an open curly bracket.</p>	29620
<p>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.</p>	
<p>Solution: The LDAP server can be configured so that a hashed password of the form {<algorithm>}hash can be passed.</p>	
<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. 	
<p>Target system synchronization does not show any information in the Manager web application.</p>	30271
<p>Workaround: Use Manager to run the target system synchronization.</p>	
<p>The following error occurs in One Identity Safeguard if you request access to an asset from the access request policy section and it is configured for asset-based session access of type User Supplied:</p>	796028, 30963
<p>400: Bad Request -- 60639: A valid account must be identified in the request.</p>	
<p>The request is denied in One Identity Manager and the error in the request is displayed as the reason.</p>	
<p>Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled.</p>	31017
<p>Cause: The SharePoint connector loads all object properties into cache by default.</p>	

Known Issue**Issue ID**

Solution:

- Correct the error in the target system.
- OR -
- Disable the cache in the file
VI.Projector.SharePoint.<Version>.Host.exe.config.

If a SharePoint site collection only has read access, the server farm account cannot read the schema properties Owner, SecondaryContact and UserCodeEnabled. 31904

Workaround: The properties UID_SPSUserOwner and UID_SPSUserOwnerSecondary are given empty values in the One Identity Manager database. This way, no load error is written to the synchronization log.

If date fields in an SAP R/3 environment contain values that are not in a valid date or time formats, the SAP connector cannot read these values because type conversion fails. 32149

Solution: Clean up the data.

Workaround: Type conversion can be disabled. For this, SAP .Net Connector for .Net 4.0 on x64, version 3.0.15.0 or later must be installed on the synchronization server.

IMPORTANT: The solution should only be used if there is no alternative because the workaround skips date and time validation entirely.

To disable type conversion

- In the StdioProcessor.exe.config file, add the following settings.
 - In the existing <configSections>:

```
<sectionGroup name="SAP.Middleware.Connector">
    <section name="GeneralSettings"
      type="SAP.Middleware.Connector.RfcGeneralConfiguration,
      sapnco, Version=3.0.0.42, Culture=neutral,
      PublicKeyToken=50436dca5c7f7d23" />
</sectionGroup>
```
 - A new section:

```
<SAP.Middleware.Connector>
    <GeneralSettings anyDateTimeValueAllowed="true" />
</SAP.Middleware.Connector>
```

There are no error messages in the file that is generated in the PowershellComponentNet4 process component, in OutputFile parameter. 32945

Cause:

No messages are collected in the file (parameter `OutputFile`). The file serves as an export file for objects returned in the pipeline.

Solution:

Messages in the script can be outputted using the `*>` operator to a file specified in the script.

Example:

```
Write-Warning "I am a message" *> "messages.txt"
```

Furthermore, messages that are generated using `Write-Warning` are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an `Exception`. This message then appears in the One Identity Manager Service's log file.

The G Suite connector cannot successfully transfer Google applications user data to another G Suite user account before the initial user account is deleted. The transfer fails because of the Rocket application's user data. 33104

Workaround: In the system connection's advance settings for G Suite, save an application transfer XML. In this XML document, limit the list to the user data to be transferred. Only run the Google applications that have user data you still need. You can see an example XML when you edit the application transfer XML in the system connection wizard.

To limit the list of user data you want to transfer

1. In the Synchronization Editor, open the synchronization project.
2. Select **Configuration > Target system**.
3. This starts the system connection wizard.
4. On the system connection wizard's start page, enable **Show advanced options**.
5. On the **Advanced settings** page, enter the XML document in the **Application transfer XML** field.
6. Save the changes.

If target system data contains appended spaces, they go missing during synchronization in One Identity Manager. Every subsequent synchronization identifies the data changes and repeatedly writes the affected values or adds new objects if this property is part of the object matching rule. 33448

Solution:

Avoid appending spaces in the target system.

Table 12: Identity and Access Governance

Known Issue	Issue ID
Moving a shelf to another shop and the recalculation tasks associated with it can block the DBQueue.	31413
<p>Solution:</p> <p>Parent IT Shop nodes of shelves and shops cannot be changed once they have been saved.</p> <p>To move a product in a shelf to another shop</p> <ul style="list-style-type: none"> • Select the task Move to another shelf. - OR - • Assign the product to a shelf in the new shop then remove the product assignment to the previous shelf. <p>Once you have moved all the products, you can delete the shelf.</p>	
During approval of a request with self-service, the Granted event of the approval step is not triggered. In custom processes, you can use the OrderGranted event instead.	31997

Table 13: Third party contributions

Known Issue	Issue ID
An 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
Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages. Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.	29051
Valid CSS code causes an error under Mono if duplicate keys are used. For more information, see https://github.com/mono/mono/issues/7455 .	762534, 762548,

Known Issue	Issue ID
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:	29607
<ul style="list-style-type: none"> • Windows Server 2016: KB4462928 • Windows Server 2012 R2: KB4462926, KB4462921 • Windows Server 2008 R2: KB4462926 	30575
<p>We do not know whether other Windows updates also cause this error.</p> <p>The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory groups during provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem.</p>	
In certain circumstances, the wrong language is used in the Stimulsoft controls in the Report Editor.	31155
<p>In the Manager web application, following errors can occur under Windows Server 2008 R2:</p> <p>System.Security.Cryptography.CryptographicException: Object was not found. at System.Security.Cryptography.NCryptNative.CreatePersistedKey (SafeNCryptProviderHandle provider, String algorithm, String name, CngKeyCreationOptions options)</p>	31995
<p>Workaround:</p> <ol style="list-style-type: none"> 1. In the Internet Information Services (IIS) Manager, select the application and then the Advanced Settings context menu item. 2. On the Process Model panel, set the option Load User Profile to True. 	
For more information, see https://support.microsoft.com/en-us/help/4014602 .	
When connecting an external web service using the web service integration wizard, the web service supplies the data in a WSDL file. This data is converted into Visual Basic .NET code with the Microsoft WSDL tools. If, in code generated in this way, default data types are overwritten (for example, if the boolean data type is redefined), it can lead to various problems in One Identity Manager.	31998
In certain Active Directory/Microsoft Exchange topologies, the Set-Mailbox Cmdlet fails with the following error:	33026

Error on proxy command 'Set-Mailbox...'

The operation couldn't be performed because object '...' couldn't be found on '...'.

For more information, see <https://support.microsoft.com/en-us/help/4295103>.

Possible workarounds:

- Connect to the Microsoft Exchange server that the user mailbox is on. Use a custom process to do this. Use the `OverrideVariables` parameter (ProjectorComponent process component) to overwrite the server (CP_ExchangeServerFqdn variable).
- Because this problem only occurs with a few schema properties, you should consider protecting these schema properties in the synchronization project against write operations. You can set the schema properties in a custom process using the `PowershellComponentNet4` process component through a user-defined Windows PowerShell call.

Schema changes

The following provides an overview of schema changes in One Identity Manager from version 8.1.3 up to version 8.1.4.

Configuration Module

- New column `QBMDBQueueTaskPerf.CountChildTasks`.

Exchange Online Module

- Columns `O3EDynDL.Notes`, `O3EMailContact.Notes`, `O3EMailUser.Notes`, and `O3EUnifiedGroup.Notes` extended to `nvarchar(1024)`.

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 8.1.3 to version 8.1.4. Apply the patches to existing synchronization projects. For more information, see [Applying patches to synchronization projects](#) on page 59.

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 27.

Table 14: Overview of synchronization templates and patches

Module	Synchronization template	Type of modification
Azure Active Directory Module	Azure Active Directory synchronization	changed
Active Directory Module	Active Directory synchronization	none
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	changed
	Oracle E-Business Suite HR data	changed
	Oracle E-Business Suite OIM data	changed
Microsoft Exchange Module	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2013/2016 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (v2)	none
	Microsoft Exchange 2013/2016/2019 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	none
Exchange Online Module	Exchange Online synchronization (deprecated)	none
	Exchange Online synchronization (v2)	none

Module	Synchronization template	Type of modification
Privileged Account Governance Module	One Identity Safeguard synchronization	none
SAP R/3 User Management 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
SharePoint Online Module	SharePoint Online synchronization	none
Universal Cloud Interface Module	SCIM Connect via One Identity Starling Connect	changed
	SCIM synchronization	changed
Unix Based Target Systems Module	Unix Account Management	none
	AIX Account Management	none

Patches for synchronization projects

The following is a list of all patches provided for synchronization projects in One Identity Manager 8.1.4. 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. Some patches are applied automatically while One Identity Manager is updating.

For more information, see [Applying patches to synchronization projects](#) on page 59.

Table 15: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#33399	Filters the members of administrator	Adds a member filter for user accounts in the vrtMember_Members property mapping rule in the DirectoryRole map.	33399

Patch ID	Patch	Description	Issue ID
	roles	This patch is applied automatically when One Identity Manager is updated.	

Table 16: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#33259_EBS	Reference scope display name	Corrects the reference scope display name	33259

Table 17: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#33476	Direction of mapping correction of Mobile phone and Business phone for guest users.	Corrects the direction of mapping for the MobilePhone and Phone schema properties in the MailUser map.	33476

Table 18: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#32347	Correction of the reference from SAP companies to SAP user accounts	Corrects resolving the reference to SAP companies in the user map for SAP S/4HANA 2.0 support.	32347
VPR#33147	Correction of SAP salutations import	Changes made in the title map to correct the import of SAP salutations and resolving references to SAP user accounts. This patch is applied automatically when One Identity Manager is updated.	33147
VPR#33423	Correction of SAP salutations provisioning	Changes property mapping rules in the title and user maps to provision SAP salutation in the correct language. This patch is applied automatically when One Identity Manager is updated.	33423

Table 19: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#33259_ SCIM	Reference scope display name	Corrects the reference scope display name	33259

Patches in One Identity Manager Version 8.1.3**Table 20: General patches**

Patch ID	Patch	Description	Issue ID
VPR#32781_ SCIM	Corrects the DefaultUserPassword variable	Corrects the security settings of the DefaultUserPassword variable. This patch is applied automatically when One Identity Manager is updated.	32781

Table 21: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#32965	Scope filter correction of ADSSite	Corrects the ADSSite's scope filters. This patch is applied automatically when One Identity Manager is updated.	32965

Table 22: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#32844	Support for domain functional level Windows Server 2016	Adds the functional level to Windows Server 2016 domains.	32844
VPR#32871	Removes the negation of TSIinheritInitial Program	Corrects the edsawTSUserConfig InheritInitialProgram in the User map because the value does not need to be negated anymore.	32871

Table 23: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#32781_ EBS	Corrects the DefaultUserPassword variable	Corrects the security settings of the DefaultUserPassword variable. This patch is applied automatically when One Identity Manager is updated.	32781

Table 24: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#32703	Allow use One Identity Manager Service user account for the connection	Allows a connection to be established using the One Identity Manager Service's user account.	32703

Table 25: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#32781_NDO	Corrects the DefaultUserPassword variable	Corrects the security settings of the DefaultUserPassword variable. This patch is applied automatically when One Identity Manager is updated.	32781

Table 26: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#32768	Correction of the Mailbox Statistics (User/Shared) mapping	Removes the Identifier <-> Identity object mapping rule from the Mailbox Statistics (User/Shared) mapping.	32768

Table 27: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#32781_SAP	Corrects the TempUserPassword variable	Corrects the security settings of the TempUserPassword variable. This patch is applied automatically when One Identity Manager is updated.	32781
VPR#33071	Change the reference scope of SAPLicence schema type (part 2)	Corrects the reference scope of the SAPLicence schema type in the One Identity Manager connection. Dependent on patch VPR#31930 (Change the reference scope of SAPLicence schema type). This patch is applied automatically when One Identity Manager is updated.	33071

Table 28: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#32899	Corrects the filter on the HRPerson_0709_IDEXT schema class	Changes the objects selection of the HRPerson_0709_IDEXT schema class. This patch is applied automatically when One Identity Manager is updated.	32899

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

Patch ID	Patch	Description	Issue ID
VPR#32754	Corrects the vrtPrimary <-> primary property mapping rule	Expands a condition on the vrtPrimary <-> primary property mapping rule in the User map.	32754

Patches in One Identity Manager version 8.1.2

Table 30: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#32258	Corrects the vrtparentDn schema property.	Corrects the property mapping rule for mapping the vrtparentDn schema property in all maps. This ensures that object properties that are not assigned a container are correctly provisioned.	32258

Table 31: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#31928	Correction of property mapping rules in the Calendar Processing (User/Shared) mapping.	Removes the mapping rule for AddNewRequestsTentatively and ProcessExternalMeetingMessages because they caused errors if they passed to the SetCalendarprocessing CmdLet.	31928

Table 32: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#32667	Deletes the alternative	Deletes the object mapping rule	32667

Patch ID	Patch	Description	Issue ID
	objects mapping rules from the oRA-Requestgroup mapping	<p>Identifier <-> REQUEST_GROUP_ID from the oRA-Requestgroup mapping.</p> <p>This patch is applied automatically when One Identity Manager is updated.</p>	
VPR#30464_1	Corrects support of Oracle Database editions	<p>Removes the CP_EBSEdition variable from the default variable set.</p> <p>This patch is applied automatically when One Identity Manager is updated.</p>	30464

Table 33: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#32031	Expose virtual appliance ID directly by the connector	<p>Sets a virtual appliance ID in the connector schema and applies it to the mappings.</p> <p>Dependent upon patch Replaces Appliance serial as appliance identifier with a custom identifier (part 2)</p> <p>This patch is applied automatically when One Identity Manager is updated.</p>	32031
VPR#32423	Introduces PAM authprovider mapping and extends the user mapping	<p>Adds a mapping and a synchronization workflow for AuthenticationProvider and corrects the User and UserGroup mappings.</p> <p>This patch is applied automatically when One Identity Manager is updated.</p> <p>IMPORTANT: Data goes missing when you apply this patch.</p> <p>To restore the data, start a full synchronization immediately after the automatic patches have been applied.</p>	32423

Table 34: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#32415	New variable for SNC login and user name and password	Adds the CP_sncsso variable to the default variable set. This patch is applied automatically when One Identity Manager is updated.	32415
VPR#32584	Change SAP title handling	Updates the connector schema so that the full SAPtitle list is loaded for each language. This patch is applied automatically when One Identity Manager is updated.	32584

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

Patch ID	Patch	Description	Issue ID
VPR#32154	Introduces some revision counters	Enables revision filtering in the Master Identity, Workdates of Employee, and Communication Data synchronization steps.	32154

Patches in One Identity Manager Version 8.1.1

Table 36: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#31456	Make User.CompanyName writeable	Removes access restrictions for the User.ComanyName schema property. CompanyName can now be written to.	31456

Table 37: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#31419	Sets rule filters for various synchronization steps in the provisioning workflow	Sets blacklist rules for group, domainDNS and builtinDomain synchronization steps in the provisioning workflow. This patch is applied automatically when One Identity Manager is updated.	31419

Patch ID	Patch	Description	Issue ID
VPR#31792	Object filter correction	Corrects object filters. This patch is applied automatically when One Identity Manager is updated.	31792

Table 38: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#31165	Use local server date as revision	Creates new connection parameters and variables for the configuration of revision filtering. By default, the local server time is used for revision filtering. Therefore, the local server time and date are applied by default.	31165
VPR#30964	Support for linked room mailboxes	This patch ensures that, in the case of LinkedRoomMailboxes, schema properties LinkedCredential, LinkedDomainController and LinkedMasterAccount are passed to the connector.	30964

Table 39: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#30269	Prevents errors when loading single objects due to identical display names	Changes the schema properties vrtModBy, vrtAcceptMessagesFrom, vrtGrantSendOnBehalfOfTo, vrtRejectMessagesFrom and all property mapping rules for these schema properties.	30269
VPR#31166	Use local server date as revision	Creates new connection parameters and variables for the configuration of revision filtering. By default, the local server time is used for revision filtering. Therefore, the local server time and date are applied by default.	31166

Table 40: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#31735	Scope filter for schema type PersonInLocality	Creates a scope filter for schema type PersonInLocality . This patch is applied automatically when One Identity Manager is	31735

Patch ID	Patch	Description	Issue ID
		updated.	
VPR#31782	Security groups definition	Correction of security groups definition. This patch is applied automatically when One Identity Manager is updated.	31782
VPR#31794	Scope filter correction	Corrects scope filters. This patch is applied automatically when One Identity Manager is updated.	31794

Table 41: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#31420	Sets rule filters for various synchronization steps in the provisioning workflow	Sets blacklist rules for Certifier and Policy synchronization steps in the provisioning workflow. This patch is applied automatically when One Identity Manager is updated.	31420

Table 42: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#31459	Mapping the AllowLinkedAccountPasswordAccess schema property.	Adds a property mapping rule for the new AllowLinkedAccountPasswordAccess schema property to the AccessRequestPolicy mapping. This patch is applied automatically when One Identity Manager is updated.	31459
VPR#31568A	Replaces Appliance serial as appliance identifier with a custom identifier (part 1)	Replaces Appliance serial as the unique identifier of the base object with a custom identifier and applies this change to the synchronization configuration. Prerequisite for patch Replaces Appliance serial as appliance identifier with a custom identifier (part 2)	31568

Patch ID	Patch	Description	Issue ID
		This patch is applied automatically when One Identity Manager is updated.	
VPR#31568B	Replaces Appliance serial as appliance identifier with a custom identifier (part 2)	<p>Replaces Appliance serial as the unique identifier of the base object with a custom identifier and applies this change to the synchronization configuration.</p> <p>Dependent upon patch Replaces Appliance serial as appliance identifier with a custom identifier (part 1)</p> <p>This patch is applied automatically when One Identity Manager is updated.</p>	31568
VPR#31569	One Identity Safeguard cluster access improvements	<p>Adds connection parameters and variables for connecting One Identity Safeguard clusters.</p> <p>This patch is applied automatically when One Identity Manager is updated.</p> <p>If you use One Identity Safeguard clusters, run the system connection wizard after applying the patch, to determine the cluster's appliances.</p>	31569
VPR#31664A	AccessRequestPolicy model changes for session access (part 1)	<p>An access request policy can have multiple directory accounts for session access.</p> <p>Prerequisite for patch AccessRequestPolicy model changes for session access (part 2).</p> <p>This patch is applied automatically when One Identity Manager is updated.</p>	31664
VPR#31664B	AccessRequestPolicy model changes for session access (part 2)	<p>An access request policy can have multiple directory accounts for session access.</p> <p>Dependent on patch AccessRequestPolicy model changes for session access (part 1).</p> <p>This patch is applied automatically when One Identity Manager is updated.</p>	31664

Patch ID	Patch	Description	Issue ID
VPR#31703	Additional rule for Director and IdentityProvider mappings	Adds an additional rule for the Directory and Identityprovider mappings. This patch is applied automatically when One Identity Manager is updated.	31703
VPR#31775A	Change to user and user group references (part 1)	Removes the reference to the directory for users and user groups and adds a reference to the authentication provider for user groups. Prerequisite for patch Change to user and user group references (part 2) . This patch is applied automatically when One Identity Manager is updated.	31775
VPR#31775B	Change to user and user group references (part 2)	Removes the reference to the directory for users and user groups and adds a reference to the authentication provider for user groups. Dependent on patch Change to user and user group references (part 1) . This patch is applied automatically when One Identity Manager is updated.	31775

Table 43: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#31412	Sets blacklist rules for provisioning	Sets blacklist property mapping rules in the user synchronization step of the provisioning workflow. This patch is applied automatically when One Identity Manager is updated.	31412
VPR#31427	Sets filter for SAPUserInSAPRole (XIsInEffect <> 0)	Creates schema class AssignmentsInEffect for schema type SAPUserInSAPRole with the filter XIsInEffect <> '0' and uses it in userInRole and userInCUARole mappings.	31427
VPR#31796	Object filter correction	Corrects object filters. This patch is applied automatically when One Identity Manager is updated.	31796
VPR#31930	Change the reference scope for the schema type SAPLicence	Corrects the reference scope of the schema type SAPLicence in the One Identity Manager connection.	31930

Table 44: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#31499	Deletes Site.NewUrl schema property	Deletes NewUrl schema property from the Site mapping. This patch is applied automatically when One Identity Manager is updated.	31499

Table 45: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#31733	Schema properties with return type request	Updates the connector schema to handle schema properties with return type request . This patch is applied automatically when One Identity Manager is updated.	31733
VPR#31756	Access token scope	Creates a scope for the access token as a new connection parameter.	31756

Patches in One Identity Manager version 8.1**Table 46: General patches**

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

Table 47: Patches for Azure Active Directory

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

Table 48: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#29087	Add the schema property mS-DS-ConsistencyGuid	Adds the schema property mS-DS-ConsistencyGuid in the User and InetOrgPerson maps.	29087

Patch ID	Patch	Description	Issue ID
VPR#29306	Schema class ADSSite (all) (part 1) correction	Changes the foreign key for ADSSite from ADSDomain to ADSFroest. Prerequisite for patch Schema class ADSSite (all) (part 2) correction . This patch is applied automatically when One Identity Manager is updated.	29306
VPR#29306_2	Schema class ADSSite (all) (part 2) correction	Changes the foreign key for ADSSite from ADSDomain to ADSFroest. Dependent on patch Schema class ADSSite (all) (part 2) correction . This patch is applied automatically when One Identity Manager is updated.	29306
VPR#30192	Scope definition and usage of processing method MarkAsOutstanding	Adds a scope and the processing method MarkAsOutstanding to the synchronization step trustedDomain.	30192
	Milestone 8.1	Milestone for the context Active Directory .	

Table 49: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#28612	Adds new property mapping rules to the Computer mapping	Adds property mapping rules for OperatingSystem, OperatingSystemVersion and OperatingSystemServicePack to the Computer mapping.	28612
VPR#29087	Add the schema property mS-DS-ConsistencyGuid	Adds the schema property mS-DS-ConsistencyGuid in the User and InetOrgPerson maps.	29087
	Milestone 8.1	Milestone for the context Active Roles .	

Table 50: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#28962_EBS	Change date conversion in script properties	A language independent format is used for converting date values in	28962

Patch ID	Patch	Description	Issue ID
		script properties. This patch is applied automatically when One Identity Manager is updated.	
VPR#29265	Extended processing methods in the synchronization step HR PersonManager	Extended the synchronization configuration EBS_Person_RemoveManager in the synchronization step HR PersonManager. This patch is applied automatically when One Identity Manager is updated.	29265
VPR#29741	Extended synchronization configuration by HR PersonPrimaryLocation	Extends a synchronization step and a mapping for synchronizing employees' primary locations.	29741
VPR#30464	Support for Oracle Database Editions	Adds a variable to the Oracle Database Edition configuration.	30464
VPR#31011	Change serialization format	Changes the serialization format of the schema types and reloaded the target system schema. This patch is applied automatically when One Identity Manager is updated.	31011
	Milestone 8.1	Milestone for the context Oracle E-Business Suite .	

Table 51: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#28815	Extends a processing method in the synchronization step RoleAssignmentPolicy	Extends the processing method MarkAsOutstanding in the synchronization step RoleAssignmentPolicy.	28815
VPR#31026	Optimizes revision filtering	Reloads the target system schema and replaces the revision counters whenChangedUTC and whenCreatedUTC with vrtRevision.	31026
	Milestone 8.1	Milestone for the context Microsoft Exchange .	

Table 52: Patches for Exchange Online

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

Table 53: Patches for G Suite

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

Table 54: Patches for LDAP

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

Table 55: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#30313	Mapping for mailbox file	Inserts a property mapping rule for access levels of mailbox files in the Person mapping.	30313

Patch ID	Patch	Description	Issue ID
	access levels		
	Milestone 8.1	Milestone for the context IBM Notes .	

Table 56: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#28147	Deletes the mapping userInMandant	Deletes the mapping userInMandant. The map is replaced by userMandant. Prerequisite for patch New mapping userMandant . This patch is applied automatically when One Identity Manager is updated.	28147
VPR#28147_2	New mapping userMandant	New mapping for accessing client user accounts (userMandant). Depends on patch Deletes the mapping userInMandant . This patch is applied automatically when One Identity Manager is updated.	28147
VPR#30453	New property mapping rule for provisioning company data	New property mapping rule for mapping user account for provisioning company data. This patch is applied automatically when One Identity Manager is updated.	30453
VPR#30941	Sets blacklist rules for provisioning	Sets blacklist property mapping rules for the userInCUARole synchronization step of the provisioning workflow. This patch is applied automatically when One Identity Manager is updated.	30941
	Milestone 8.1	Milestone for the context SAP R/3 .	

Table 57: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#29265	Extends a processing method in the synchronization step Managers	Extended the processing method SHR_Department_RemoveManager in the synchronization step Managers This patch is applied automatically	29265

Patch ID	Patch	Description	Issue ID
		when One Identity Manager is updated.	
	Milestone 8.1	Milestone for the context SAP R/3 structural profile add-on .	

Table 58: Patches for SAP R/3 BI analysis authorizations

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

Table 59: Patches for SAP R/3 authorization objects

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

Table 60: Patches for SharePoint

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

Table 61: Patches for SharePoint Online

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

Table 62: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#30497	Allows configuration of local cache	Adds a variable for disabling use of local cache. This patch is applied automatically when One Identity Manager is updated.	30497
VPR#31250	Corrections to the scripts of virtual schema properties	Adds a NULL value test in the get scripts of virtual schema properties. This patch is applied automatically when One Identity Manager is updated.	31250
	Milestone 8.1	Milestone for the context SCIM .	

Table 63: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)

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

Table 64: Patches for Unix

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

Table 65: Patches for the One Identity Manager connector

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

Table 66: Patches for the CSV connector

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

Deprecated features

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

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

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

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

- Google ReCAPTCHA Version 1 is no longer supported.
- The process component SvnComponent has been removed.
- The **Common | MailNotification | DefaultCultureFormat** configuration parameter has been deleted.

Customized usage might require modification. The language for formatting values is determined through the current employee.

- The following scripts have been removed because their functions are obsolete or no longer ensured:
 - VI_Del_ADSSAccountInADSGroup
 - VI_GetDNSHostNameOfHardware
 - VI_GetDomainsOfForest
 - VI_GetServerFromADSContainer
 - VI_Make_Ressource
 - VID_CreateDialogLogin
 - VI_Discard_Mapping
 - VI_Export_Mapping
 - VI_GenerateCheckList
 - VI_GenerateCheckListAll

The following functions are discontinued in future versions of One Identity Manager and should not be used anymore.

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

Identity Manager schema.

- In future, the **viITShop** system user will not be supported and will be deleted. Use role-based login with the appropriate application roles.
- In future, the `VI_BuildPwdMessage` script will not be supported and will be deleted.

Mail templates are used to send email notifications with login information. The mail templates are entered in the **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** and **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameters.

System requirements

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

Minimum requirements for the database server

Processor	8 physical cores 2.5 GHz+ NOTE: 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM
Hard drive storage	100 GB
Operating system	Windows operating system <ul style="list-style-type: none">• Note the requirements from Microsoft for the SQL Server version installed. UNIX and Linux operating systems <ul style="list-style-type: none">• Note the minimum requirements given by the operating system manufacturer for SQL Server databases.
Software	Following versions are supported: <ul style="list-style-type: none">• SQL Server 2016 Standard Edition (64-bit), Service Pack 2 with the current cumulative update• SQL Server 2017 Standard Edition (64-bit) with the current

cumulative update

- SQL Server 2019 Standard Edition (64-bit) with the current cumulative update

NOTE: The cumulative update 2 for SQL Server 2019 is not supported.

- 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 strongly recommended on performance grounds.

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 2019• Windows Server 2016• Windows Server 2012 R2• Windows Server 2012• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later Linux operating system <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 4.7.2 or later <p>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 5.14 or later

Minimum requirements for clients

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

Minimum requirements for the Web Server

Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating system <ul style="list-style-type: none">• Windows Server 2019• Windows Server 2016• Windows Server 2012 R2• Windows Server 2012• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later Linux operating system <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 4.7.2 or later
- Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and Role Services:
 - Web Server > Common HTTP Features > Static Content
 - Web Server > Common HTTP Features > Default Document
 - Web Server > Application Development > ASP.NET
 - Web Server > Application Development > .NET Extensibility
 - Web Server > Application Development > ISAPI Extensions
 - Web Server > Application Development > ISAPI Filters
 - Web Server > Security > Basic Authentication
 - Web Server > Security > Windows Authentication
 - Web Server > Performance > Static Content Compression
 - Web Server > Performance > Dynamic Content Compression

Linux operating system

- NTP - Client
 - Mono 5.14 or later
 - Apache HTTP Server 2.0 or 2.2 with the following modules:
 - mod_mono
 - rewrite
 - ssl (optional)
-

Minimum requirements for the Application Server

Processor 8 physical cores 2.5 GHz+

Memory 8 GB RAM

Hard drive storage 40 GB

Operating system Windows operating system

-
- Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
 - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later

Linux operating system

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

Additional Windows operating system software

- Microsoft .NET Framework Version 4.7.2 or later
- Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and Role Services:
 - Web Server > Common HTTP Features > Static Content
 - Web Server > Common HTTP Features > Default Document
 - Web Server > Application Development > ASP.NET
 - Web Server > Application Development > .NET Extensibility
 - Web Server > Application Development > ISAPI Extensions
 - Web Server > Application Development > ISAPI Filters
 - Web Server > Security > Basic Authentication
 - Web Server > Security > Windows Authentication
 - Web Server > Performance > Static Content Compression
 - Web Server > Performance > Dynamic Content Compression

Linux operating system

- NTP - Client
 - Mono 5.14 or later
 - Apache HTTP Server 2.0 or 2.2 with the following modules:
 - mod_mono
 - rewrite
 - ssl (optional)
-

Supported data systems

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

Table 67: Supported data systems

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.
Connector for relational databases	Any relational databases supporting ADO.NET. NOTE: Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer.
Generic LDAP connector	Any LDAP directory server conforming to version 3. The LDAP connector requires the directory server to be RFC conform. Specifically, to conform to the standards RFC 4514 (String Representation of Distinguished Names) and RFC 4512 (Directory Information Models). NOTE: Other schema and provisioning process adjustments can be made depending on the schema.
Web service connector	Any SOAP web service providing wsdl. NOTE: You can use the Web Service Wizard to generate the configuration to write data to the Web Service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active Directory connector	Active Directory, shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.
Microsoft Exchange connector	<ul style="list-style-type: none"> • Microsoft Exchange 2010 Service Pack 3 or later • Microsoft Exchange 2013 with cumulative update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange hybrid environments
SharePoint connector	<ul style="list-style-type: none"> • SharePoint 2010 • SharePoint 2013 • SharePoint 2016 • SharePoint 2019
SAP R/3	<ul style="list-style-type: none"> • SAP Web Application Server 6.40

Connector Supported data systems

connector	<ul style="list-style-type: none">• SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, and 7.69• SAP ECC 5.0 and 6.0• SAP S/4HANA On-Premise-Edition
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the Authentication Services specifications.
IBM Notes connector	<ul style="list-style-type: none">• IBM Domino Server versions 8, 9, and 10• HCL Domino Server version 11• IBM Notes Client 8.5.3 and 10.0• HCL Notes Client Version 11.0.1
Native database connector	<ul style="list-style-type: none">• SQL Server• Oracle Database• SQLite• MySQL• DB2 (LUW)• CData ADO.NET Provider• SAP HANA
Mainframe connector	<ul style="list-style-type: none">• RACF• IBM i• CA Top Secret• CA ACF2
Windows PowerShell connector	<ul style="list-style-type: none">• Windows PowerShell version 3 or later
Active Roles connector	<ul style="list-style-type: none">• Active Roles 6.9, 7.0, 7.2, 7.3.1, 7.3.3, 7.4.1 and 7.4.3
Azure Active Directory connector	<ul style="list-style-type: none">• Microsoft Azure Active Directory <p>NOTE: There is no support for synchronizing Microsoft Azure China using the Azure Active Directory connector. For more information, see https://support.oneidentity.com/KB/312379.</p>
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0.
Exchange	<ul style="list-style-type: none">• Microsoft Exchange Online

Connector Supported data systems

Online connector

G Suite connector

- G Suite

Oracle E-Business Suite connector

- Oracle E-Business Suite System versions 12.1 and 12.2

SharePoint Online connector

- Microsoft SharePoint Online

One Identity Safeguard connector

- One Identity Safeguard Version 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 and 6.0

Product licensing

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

Upgrade and installation instructions

To install One Identity Manager 8.1.4 for the first time, follow the installation instructions in the *One Identity Manager Installation Guide*. For more detailed instructions about updating, see the *One Identity Manager Installation Guide*.

| IMPORTANT: Note the [Advice for updating One Identity Manager](#) on page 53.

Advice for updating One Identity Manager

- Ensure that the administrative system user, who is going to compile the database, has a password before you update the One Identity Manager database to version 8.1.4. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:

- Automatic software updating of version 7.0 to version 8.1.4 only works smoothly if the service pack 7.0.3 is installed. In addition, the files VI.Update.dll and JobService.dll must be installed.

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

To distribute the file, use the Software Loader.

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

- Automatic software updating of version 7.1 to version 8.1.4 only works smoothly if the service pack 7.1.3 is installed.
- One Identity Manager uses In-Memory OLTP ((Online Transactional Processing) for memory optimized data access. The database server must support Extreme Transaction Processing (XTP). If XTP is not enabled, the installation or update will not start. Check whether the SQL Server property **Supports Extreme Transaction Processing** (IsXTPSupported) is set to **True**.

The following prerequisites must be fulfilled to create memory-optimized tables:

- A database file with the file type **Filestream data** must exist.
- A memory-optimized data filegroup must exist.

The Configuration Wizard checks whether these prerequisites are fulfilled before the One Identity Manager database can be installed or updated. The Configuration Wizard offers repair methods for creating the database file and database group.

- During the update of a One Identity Manager database version 7.0, 7.1 or 8.0 to version 8.1.4, different columns that were already semantically defined as mandatory fields become physical mandatory fields.

During the schema update with the Configuration Wizard, errors may occur due to inconsistent data. The update quits with an error message.

```
<table>.<column> must not be null
Cannot insert the value NULL into column '<column>', table '<table>';
column does not allow nulls.
UPDATE fails
```

Check and correct data consistency before updating a One Identity Manager database. In the add-on for the Configuration Module on the installation medium, a test script (\SDK\SQLSamples\Files\MSSQL2K\30374.sql) is provided. In case it fails, correct the data and restart the update.

- During installation of a new One Identity Manager database or a new One Identity Manager History Database with version 8.1.4 or while updating an One Identity Manager database or One Identity Manager History Database from version 7.0.x, 7.1.x or 8.0.x to version 8.1.4, you can specify whether you want to work with granular permissions at server and database level. The Configuration Wizard then creates SQL Server logins and database users with the necessary permissions for administrative user, configuration users and end users. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

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

If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to <https://support.oneidentity.com/identity-manager/>.

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

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

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


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

```
sc delete "HDBService"
```

Updating One Identity Manager to version 8.1.4

| IMPORTANT: Note the [Advice for updating One Identity Manager](#) on page 53.

To update an existing One Identity Manager installation to version 8.1.4

1. Run all the consistency checks in the Designer in **Database** section.
 - a. Start the Consistency Editor in the Designer by selecting the **Database > Check data consistency** menu item.
 - b. In the **Test options** dialog, click .
 - c. Under the **Database** node, enable all the tests and click **OK**.
 - d. To start the check, select 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: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.

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

(From version 8.0.x or version 8.1.x). End the One Identity Manager Service on the update server.

4. Make a backup of the One Identity Manager database.
5. Check whether the database's compatibility level is set to **130** and change the value if required.
6. Run the One Identity Manager database schema update.

- Start the Configuration Wizard on the administrative workstation and follow the instructions.

Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.

- Use the same user as you used for initially installing the schema.
- If you created an administrative user during schema installation, use that one.
- If you selected a user with Windows authentication to install the schema, you must use the same one for updating.

NOTE: If you want to switch to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to version 8.1.4, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

If you want to switch to granular permissions when you update from 8.1.x to version 8.1.4, contact support. To access the Support Portal, go to <https://support.oneidentity.com/identity-manager/>.

7. (From version 7.0.x or version 7.1.x) Update the One Identity Manager Service on

the server that processes direct database queries.

(From version 8.0.x or version 8.1.x). Update the One Identity Manager Service on the update server.

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

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

- c. Click **Install**.

This starts the installation wizard.

- d. Follow the installation instructions.

IMPORTANT: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.

NOTE: After updating a One Identity Manager History Database installation from version 7.0.x or Version 7.1.x, the One Identity Manager History Service is not registered.

Register the service manually. Run the following command on the command line in administrative mode:

```
sc create "HDBService" binpath= "<path>\vinetworkservice.exe"  
displayname= "One Identity Manager History Service"  
  
sc description "HDBService" "One Identity Manager History Service"
```

8. Check the login information of the One Identity Manager Service. Revert to the original settings if the One Identity Manager Service did not initially use the local system account for logging in. Specify the service account to be used. Enter the service account to use.
9. Start the One Identity Manager Service on the update server.
10. Update other installations on workstations and servers.

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

To update synchronization projects to version 8.1.4

1. If you have set up synchronization projects for connecting cloud applications in the Universal Cloud Interface, update the target system schema in these synchronization projects using the Synchronization Editor.
2. Any required changes to system connectors or the synchronization engine are made available when you update One Identity Manager. These changes must be applied to existing synchronization projects to prevent target system synchronizations that are already set up, from failing. Patches are made available for this.

NOTE: Some patches are applied automatically. A process that migrates all

existing synchronization project is queued in the Job queue to do this. To execute the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

- Check whether the `DPR_Migrate_Shell` process has been started successfully.
If the patch cannot be applied because the target system could not be reached, for example, you can manually apply it.

For more information, see [Applying patches to synchronization projects](#) on page 59.

To update an application server to version 8.1.4

- After updating the One Identity Manager database's schema, the application server starts the automatic update.
- To start the update manually, open the application's status page in the browser and select **Update immediately** from the current user's menu.

To update the Web Portal to version 8.1.4

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 instructions, see the *One Identity Manager Installation Guide*.

To update an API Server to version 8.1.4

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

To update the Operations Support Web Portal to version 8.1.4

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

To update the Manager web application to version 8.1.4

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 alter custom changes in synchronization projects. This means that conflicts may occur if patches are applied to synchronization projects that have been customized. It may cause loss of data.

Before you apply a patch

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

NOTE: If you update existing synchronization projects, the connection parameters from the default variable set are always used. Ensure that the variables in the default variable set contain valid values.

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

To apply patches

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

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

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

See also:

- [Modified synchronization templates](#) on page 26
- [Patches for synchronization projects](#) on page 27

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 2019.0001.0021.0400 for all modules and the application version 8.1 2019-01-21-396 verify that this version is installed.

Additional resources

Additional information is available from the following:

- [One Identity Manager Support](#)
- [One Identity Manager Online documentation](#)
- [One Identity Manager Community](#)
- [One Identity Manager Training portal website](#)

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

Copyright 2020 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 highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**