One Identity Manager 8.1.2

Release Notes

February 2020

These release notes provide information about the One Identity Manager release, version 8.1.2. You will find all the modifications since One Identity Manager version 8.1.1 listed here.

One Identity Manager 8.1.2 is a patch release with new functionality and better behavior. See New features on page 2 and Enhancements on page 4.

If you are updating a One Identity Manager version older than One Identity Manager 8.1.1, 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

About One Identity Manager 8.1.2

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 8.1.2:

Basic functionality

- Support for SQL Server 2019 with the compatibility level for databases **SQL Server 2016 (130)**.
- As from One Identity Manager version 8.1.2, a new method is available for updating customer databases faster. This method is only implemented for updating the schema in the context of service packs. For initial schema installation and updating the schema to a new main version, the conventional method is still used.

  NOTE: This method is applied to schema updates as from One Identity Manager version 8.1.2 assuming version 8.1.1 is installed. Updating of older One Identity Manager versions to version 8.1.2 uses the conventional method.
- Support for custom staging levels for the One Identity Manager database. This information is shown in the status bar of the programs in the database connection tooltip and in the installation overview in the Launchpad.

Web applications

- In the Web Portal, you can display and request products that other people from your vicinity have already requested. As a manager, you can also see products from your team's peer groups.
- In the Web Portal, you can specify how dates and numbers are formatted. You can configure this in the **My Profile | Contact Data | Language for value formatting** field.
- You can configure the Password Reset Portal such that you can log in using user accounts other than the central user account with help of password questions or a passcode (for example, with the name of the Active Directory user account). Use the **QER | Person | PasswordResetAuthenticator | DisabledBy**, **QER | Person | PasswordResetAuthenticator | EnabledBy**, **QER | Person | PasswordResetAuthenticator | SearchColumn**, and **QER | Person | PasswordResetAuthenticator | SearchTable** configuration parameters to configure this. For more detailed information, see the *One Identity Manager Web Application Configuration Guide*.

Target system connection

- One Identity Safeguard Version 2.8, Version 2.9, Version 2.10, and Version 2.11. are supported.
- Microsoft Exchange 2013 with cumulative update 23 is supported.
- **TECH PREVIEW ONLY**: A new LDAP connector **LDAP Connector (Version 2 - Tech Preview)** is available. Project templates are made available for OpenDJ, Active Directory Lightweight Directory Services (AD LDS), and Oracle Directory Server Enterprise Edition (DSEE) as well as a generic project template. The connector can be tested in a test environment. You must definitely not use the connector in a live environment.

Identity and Access Governance

- Use the **QER | Person | UseCentralPassword | CheckAllPolicies** configuration parameter to specify if an employee's central password is checked against all the target system's password policies of the employee's user accounts. Checking is only carried out in the Password Reset Portal.
- Approvers that are registered for Starling Two-Factor Authentication, can also use the Starling 2FA app for approvals. This option is available if you use Starling Cloud for multi-factor authentication. Use the **QER | Person | Starling | UseApprovalAnywhere** and **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** configuration parameters to configure the required behavior.
- Support for peer group analysis for attestation.

  There is a new `PeergroupAnalysis` event for the `AttestationCase` table that you can link into the approval workflow with an EX step. In this approval step, whether the attestation case is automatically granted or denied approval depends on a peer group analysis of the employee connected to the attestation object. The peer group analysis

is determined through the manager or department of the employee connected to the attestation object.

To configure peer group analysis for attestation, use the **QER | Attestation | PeerGroupAnalysis** configuration parameter and its subparameters.

See also:

- Enhancements on page 4
- Resolved issues on page 8
- Schema changes on page 27
- Patches for synchronization projects on page 29

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.1.2.

Table 1: General

Enhancement	Issue ID
Improved performance transferring deleted Job queue entries to the process history.	31103, 32402
Improved performance of DBQueue Processor tasks for shrinking records from process monitoring and the process history.	31954
Improved performance processing DBQueue Processor tasks with large amounts of data.	32146
Improved performance processing DBQueue Processor tasks during synchronization. To prevent possible blocking of DBQueue Processor task processing during synchronization, a DBQueue buffer (QBMDBQueuePond table) is implemented. The time period for deferring remaining entries is defined in the **QBM | DBQueue | BufferTimeout** configuration parameter (default **120** minutes).	32525, 32577
Improved performance deleting objects including all their dependencies.	32223
Improved performance executing deferred operation with large amounts of data.	32373
Improved performance updating current UTC offsets of all timezones.	32567
Columns that need to be in a defined display pattern in the table are given implicit viewing permissions.	31143
Improved compilation of HTML applications in the Configuration Wizard.	32050

Enhancement	Issue ID
Improved documentation for applying scripts about conditional displaying and editing of columns. For more detailed information, see the *One Identity Manager Configuration Guide*.	32540
Improved how to determine the current version of the database server to display in the system configuration report.	32139
Improved accessing the One Identity Manager History Database when connected through an application server. When you install an application server, you can enter the connection data to one or more One Identity Manager History Databases. You can also enter an One Identity Manager History Database's connection data at a later date. To do this, change the application server's configuration file (`web.config`). For detailed information, see the *One Identity Manager Installation Guide* and the *One Identity Manager Operational Guide*.	32317
New consistency checks test whether or not there is a deferred operation that has already been triggered but does not have a process in the Job queue.	32218
Improved the **Objectkey references to non existing object** and **Objectkey references to non existing object (tolerated)** consistency checks.	31898, 32197, 32333
You can specify a priority for registering a customizer method. If serveral methods of the same name are found, the method with the highest priority is selected. Therefore, methods from other customizers can be overwritten, if permitted.	32355
The **Fallback connection** option (`QBMConnectionInfo.IsFallBackAppServer`) for the process generation connection data can only be enabled for one application server.	32414
Improved identification of expiring sessions on the application server.	31719
Improved reestablishing connections to the application server.	32485
Improved protection against damaging SQL statements.	31768, 32102, 32285
Improved error messages when transporting changes if an error occurs while implementing them in the target database.	32022
New `MergeAction` parameter in the `DBTransporterCMD.exe` command line program for handling merge conflicts during a transport.	32027
The `ScriptComponent` process component has two new process functions available to it, `ScriptExecExclusive` and `ScriptExecExclusive32`, for executing scripts exclusively for one object.	32562

Enhancement	Issue ID
Improved accessibility in the Manager.	32157
Improved how permitted and not permitted character classes for password policies are displayed on forms in the Manager and the Designer.	32205
Improved how translations are displayed in the **Edit translation** dialog.	32216

Table 2: General web applications

Enhancement	Issue ID
Improved security for dealing with column filters in the Web Portal.	32192
Improved performance making approval decisions for request and attestations in the Web Portal.	32220
Improved performance of certain database queries in the Web Portal.	32253
Removed checkbox in front of the date field in the Web Portal. If you do not want a time restriction, do not enter anything in the field.	801120
When an API is compiled, it is tested to see if a `ConfigureAwait(false)` method has been used for each `await` keyword. This ensures that asynchronous code is applied correctly.	803817
Webauthn security keys: The RSTS version has been updated to version 2019.11.22.0. You can prevent the **X-Frame-Options** HTTP response header from being returned by setting the **DisableAddingXFrameOptionsHeader** configuration setting to **true**.	803934
Improved performance of grid controls. Less database queries are generated.	806371
The Web Portal monitor page has been reworked and now shows better information.	803262
Improved performance of database-bound grids.	32393
In the Web Portal, the system role’s Hyper View has been reworked.	20188
On the Web Portal's start page, assignment resources, multi-requestable/unsubscribable resources, and resources are now visible in the **My Responsibilities** tile.	31934
Improved performance displaying requestable products in the Web Portal.	32057
Improved performance requesting products in the Web Portal.	32255

Table 3: Target system connection

Enhancement	Issue ID
Only relevant project templates are offered in the project wizard.	25471
Synchronization of objects with incorrect object properties can be allowed if necessary.	31722
Improved performance synchronizing Microsoft Exchange recipient lists.	31163
The Oracle E-Business Suite connector recognizes on its own, which Oracle Database Editions are used in the target system. A patch with the patch ID VPR#30464_1 is available for synchronization projects.	30464
Improved performance provisioning assignments of Oracle E-Business Suite entitlements to user accounts.	32498
During provisioning of G Suite user accounts, user accounts are prevented from being processed in parallel.	32320
During provisioning of Notes objects, the latency is increased after the index is refreshed to be able to reload object properties without errors.	32448
In the One Identity Safeguard connector, the version of the Windows PowerShell module in use is checked to see if it is supported and matches the appliance. If this is not the case, the connection is closed with an appropriate error message.	32425
Support for Telnet session request for PAM.	32544
The SAP connector now uses SAP code pages 6100, 6200, and 6500.	32118
Accelerated synchronization of personnel planning data from an SAP HCM system. A patch with the patch ID VPR#32154 is available for synchronization projects.	32154
New USOBHASH schema type in the SAP connector schema to load permissions from the USOBHASH table in SAP R/3.	32292
The SCIM connector now allows parallel access 10 times max. to load single objects during synchronization.	32564
Improved performance using the SCIM connector for synchronization.	32599
The CSV connector now takes language settings into account when reading and writing.	32000

Table 4: Identity and Access Governance

Enhancement	Issue ID
When a passcode is created, it is logged in the system journal.	31945
Business roles that are used in assignments resources cannot be deleted anymore.	31806
Improved performance calculating `QER_FTPWOVisibleForPerson`.	32045, 32334
The **Retain service item assignment on relocation** option can now be set on default service items.	32588

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 29

Resolved issues

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

Table 5: General known issues

Resolved issue	Issue ID
The following error occurs while the One Identity Manager database is updating from version 7.0.x, 7.1.x, or 8.0.x to version 8.1.1: `Database error 41337: Cannot create memory optimized tables. To create memory optimized tables, the database must have a MEMORY_OPTIMIZED_FILEGROUP that is online and has at least one container.`	31981
The schema update fails on `QBM_PIndexDropRedundant` if there are indexes with a lot of columns.	32569
In the Configuration Wizard, changing to a new login for an administrative user when installing a One Identity Manager database does not work correctly. This happens if the database connection was established with Windows authentication.	32074
In the Configuration Wizard, an error occurs selecting the directory for database files in the file browser if an installation user with granular permissions is used and the files are not stored in the database server's default directories. For more information about the required authorizations, see the *One Identity*	32274

Resolved issue	Issue ID
Manager Installation Guide.	
Custom files are deleted during update installation of local assemblies.	28985
Backup files are sometimes generated in the wrong directory during an One Identity Manager update.	32232
Web application assemblies are not completely deleted during compilation.	32201
Errors when the `RemoteConnectPlugin` starts are not properly logged in the One Identity Manager Service.	32208
Error querying if the SQL Server Agent is running on an Azure SQL Database.	32371
In the search index, the change date is set even though a table is not indexed in a run.	32406
On a server with AlwaysOn availability groups, if a One Identity Manager History Database is not in an AlwaysOn availability group, data is not transferred to the One Identity Manager History Database.	31721
Error if the name of the connection server for transferring data to the One Identity Manager History Database contains special characters.	32163
When a connection server is created, data transfer to a One Identity Manager History Database fails if the **is_rpc_out_enabled** option is not set.	32492
Error describing the SPML test front-end configuration.	31728
In certain circumstances, the compiler dialog box is not displayed when transporting change labels, even though compilation is required.	31868
Importing the transport package sometimes does not complete.	32025
If a process step fails, the execution status of the following process step is correctly set to **False** however subsequent steps retain the execution status **Loaded**. This means that no more process steps are handled for this process.	32020
It is not possible to create schedules with a long interval because the start date is skipped.	32047
If a script being executed over the `Execute Script` process task of the `PowerShellComponent` process component fails, passwords contained in the script are written out in the One Identity Manager Service's log.	32089
Error adding objects to change labels.	32159, 32160
Errors in the `SDK_IPasswordManager_CreatePassword` and `SDK_IPasswordManager_ValidatePassword` scripts. The scripts determine password policies without a base object.	32193

Resolved issue	Issue ID
Changing an MVP column that is configured for logging changes, does not generate a recalculation task for `Watch*` trigger.	31989
Blockages of the `QBMDBQueueCurrent` table cause performance problems during processing of certain DBQueue Processor tasks. In this context, there is a new consistence check called **Custom defined Z-Procedure without corresponding R-Procedure**.	32087
In certain circumstances, post-processing are not generated.	32194
In certain circumstances, an error occurs in the `QBM_PDBQueueProcess_Del` procedure.	32332
The dialog for editing report master data in the Report Editor can be opened twice at the same time.	32202
Internal temporary table for determining historical data for reports is created with the wrong sort order.	32555
Identity providers (`QBMIdentityProvider` table) cannot be created in the Designer.	32209, 32431
Error opening the process plan editor if the Designer is running in quick edit mode.	32230
The `ResolveImportValueHashed` function cannot handle dynamic foreign keys.	32214
Error evaluating scripts about visibility (`DialogColumn.CanSeeScript`).	32239
The `QBM_PUserDetectByGroupList` procedure removes too many permissions groups.	31601, 32068
During migration of One Identity Manager version 8.0.x to 8.1.x, the foreign key columns' edit permissions are not cleared up if they come from custom permissions groups.	29031, 32270, 32352
Permissions missing during process simulation.	32495
The `DynamicGroup.Displayname` column is too short.	32273
Error passing the entity in the script (`LineScriptName` parameter) in the `ScriptComponent` process component's `CSVExport` process task.	32409
In the Schema Extension, permissions for database view are not tested correctly.	32065
The Schema Extension wizard does not display all the error messages that occur when custom schema extensions are deleted.	32413
Custom table of **ReadOnly** type are not generated correctly.	32464
The **_Old** suffix causes errors during bulk updating of column names.	32488

Resolved issue	Issue ID
In the Manager, error loading historical data in the TimeTrace view.	32283
An error occurs in a date field if the value larger than **31.12.9998** is entered.	32368
In certain circumstances, objects in the Manager are opened as read-only.	32417
Incorrect sorting of date values in the Manager if **English (USA)** is set as the language.	32441
In the Filter Designer, searching with **Ctrl + F** does not work properly.	32552
Inaccurate calculation of the memory required on a server.	32199
In certain circumstances, table relations are incorrectly identified as errors in the consistency check.	32443
In certain circumstances, entries in `QBMElementAffectedByJob` are not processed.	32534
In the `DBTransporterCMD.exe` command line program, background processes are not correctly taken into account during testing to see if single user mode can be enabled.	32601
In certain circumstances in the `DBTransporterCMD.exe` command line program, single user mode is not exited.	32620
Insufficient references in certain scripts.	32644

Table 6: General web applications

Resolved issue	Issue ID
In the Web Portal, you cannot delete bookmarks referencing objects that no longer exist. Now you can delete bookmarks in a tile on the Web Portal`s start page.	31912
In the Web Portal, on the employee history page, it is not possible to sort the table without setting a filter beforehand.	31938
In the Web Portal, an error occurs if, within one session, a new subgroup is added to an Active Directory group and another subgroup is added under the first subgroup.	31940
In the Web Portal, the **Back** button on the **Pending attestations** page only works if there are no attestations.	31963
In the Web Portal, if you temporarily deactivate an employee, an error occurs if the current date is selected in **Temporarily disabled until**.	31967
In the Web Portal, you can sort by columns with hidden content.	31969
In certain circumstances in the Web Designer, an object is loaded without the mandatory column `XObjectKey`.	31971

Resolved issue	Issue ID
In the Web Designer, if the value of **Minimum number of characters** is set to less than 1025 characters in the copy or extension of a particular component (for example, **VI_UNS_RequestNewGroup**), then only a maximum of 1024 characters can be entered in this field in the Web Portal at a later date.	31980
In the Web Portal, the **Send a reminder mail** dialog does not have a scroll bar.	31992
In the Web Portal, an error occurs if a report is shown that requires input of a value for a parameter.	32004
In certain circumstances in the Web Portal, filtering requesters in the request history causes an error.	32006
In certain circumstances in the Web Portal, an approver of an attestation case cannot analyze the removal of permissions.	32012
In certain circumstances, single sign-on does not work for the API Server.	32017
In the Web Portal, displaying request queries takes a long time.	32018
In the Web Portal, if a filter is applied to both the **Request** column and the **Product** column, the results do not correspond to the filters anymore and too many results are displayed.	32019
In the Web Portal, the **Pending requests** page takes too long to show the pending requests.	32023
In the Web Portal, if you search while system entitlements are displayed, an error occurs.	32024
In the Web Portal, an error occurs while searching for products for a new request.	32066
In the Web Portal, searching on the **Auditing - Requests** page does not return all the results.	32069
When business roles are displayed in the Web Portal with Internet Explorer 11, the manager and deputy are missing.	32140
If the **Hardware** configuration parameter is not set, no more requests can be made in the Web Portal.	32144
In the Web Portal, displaying entitlements for staff, takes a long time.	32178
In the Web Designer, if a logo is selected for the login screen, an error occurs.	32269
In the Web Portal, an error occurs if several requests are selected and approved at the same time.	32312
If the Web Portal login through OAuth 2.0/OpenID Connect fails, the browser hangs.	32316

Resolved issue	Issue ID
In the Password Reset Portal, the **View settings | Select all** option is not applied to all the lists shown.	32340
In certain circumstances, the Web Portal shows unsaved changes to user data until the user logs in again.	32358
In the Web Designer, an error occurs if a project is compiled that contains a combobox (node) that does go through any iterations.	32366
In the Web Portal, selecting an employee for a new request can take a long time.	32372
In the Web Designer, some Web SQL functions cannot be used in conditions in column lists.	32374
In the Web Portal's mobile view, dialogs and their content as well as button texts are not completely displayed.	32379, 32386
In the Web Portal, the **Disabled until** field shows the wrong date in the employee's master data.	32440
In certain circumstances in the Web Portal, multi-select buttons (without any function) are sometimes displayed for pending attestation cases.	32445
Use of the **|** character in the password of the SQL user who was used to install a web application causes and error.	32461
In certain circumstances in the Web Portal, the shopping cart check shows incorrect results.	32483
In the source of an export file created by the Web Portal, you can see a full path.	32523
In the Web Portal, an error message wrongly displays an HTML tag when the shopping cart is being checked.	32529
In the Web Portal, dependent applications are not sorted in the menu.	32639
In certain circumstances in the Web Portal, an attestor does not have sufficient permissions to analyze the removal of permissions.	206529
In the Manager web application, an error occurs selecting an assigned object on a system role's overview form.	31949
In the Manager web application, the icons in the menus are not shown correctly.	31960
In the Manager web application, an error occurs displaying rule violations.	32304

Table 7: Target system connection

Resolved issue	Issue ID
Synchronization projects cannot be opened after importing because dependencies are missing.	31876
Error synchronizing if the value of a schema property for resolving keys contains more than one $ character. The connector handles this value as a variable.	31964
In the synchronization log, objects that are marked as outstanding, are not logged.	32011
Incorrect result if account definition assignments are deleted for an employee and then added again shortly afterward.	32063
Error provisioning group memberships if there are schema properties that are not mapped in the mapping to be executed.	32077
Provisioning processes are not generated if the mapping in use references a base map and the base map is not used in the provisioning workflow.	32152
Error during synchronization: `This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.`	32177
When you close a synchronization project, the password for logging in to the target system is saved incorrectly if it contains the dollar ($) character.	32226, 32311
Objects with a combined primary key with a value of `timestamp`, cannot be reloaded.	32266
If single provisioning of memberships is disabled, changes to memberships are not provisioned if a value comparison rule is used.	32280
Special characters are not masked correctly in custom project templates.	32474
Error during synchronization: `The connection does not support MultipleActiveResultSets.`	32604
Error creating synchronization projects with the Synchronization Editor Command Line Interface if there is a special character in the connection parameter.	32496
On the form for defining search criteria for employee assignment, the allocated base object's UID is display instead of the user account's UID. This happens if the display pattern for the user account table is made up of several columns.	32612
If an error occurs loading the object list, the SCIM connector returns an empty list as successfully loaded. The error only occurs in One Identity Manager version 7.1.x and 8.0.x.	32646

Resolved issue	Issue ID
In certain circumstances, Active Directory objects are marked as outstanding or deleted during synchronization but the marker is immediately removed again.	31908
On the form for assigning Active Directory groups to an Active Directory user account, groups are shown that are marked as only for use in the IT Shop.	31944
When an Active Directory user account is added, it is possible to enter a different primary group to that of **Domain Users**.	32061
If only upper and lower case changes in the display name of an Active Directory object, the change is not provisioned.	32091
If a double s changes to sz (ß) changes in the display name of an Active Directory objects, the change is not provisioned.	32112
The LDAP search filter for finding Active Directory objects is set up incorrectly. This means it finds too many objects. Only after the objects from all object classes have been loaded does the filter run again with the correct object classes, effectively recalculating the object list correctly. However because too many objects were loaded in the first place, synchronization takes longer.	32166
If a container is deleted from an Active Directory user account, verification of the object properties fails after provisioning. A patch with the patch ID VPR#32258 is available for synchronization projects.	32258
The formatting script for `ADSDomain.ADSDomainName` causes an error.	32275
Some assignment forms for Active Directory objects can be opened with multi-select.	32438
Error provisioning Oracle E-Business Suite objects.	32430
E-Business Suite request groups are not synchronized if the `REQUEST_GROUP_ID` is identical. A patch with the patch ID VPR#32667 is available for synchronization projects.	32667
The G Suite connector cannot load more than 1000 G Suite product and SKU assignments.	32128
Error loading the Notes schema when setting up synchronization if there is a Notes group that apparently has corrupt attributes.	32237
Setting up and executing synchronization with IBM Notes fails if Notes Views are saved with a different name in the Domino directory.	32471
The Notes connector returns the wrong value for `AdminRequest,Type`.	32589
Error changing the certificate of a Notes user account.	32605

Resolved issue	Issue ID
Error publishing changes to Exchange Online mailboxes in the **Calendar Processing (User/Shared)** synchronization step. A patch with the patch ID VPR#31928 is available for synchronization projects.	31928
Exchange Online objects with a single quote (') in their name cannot be synchronized.	32514
Single object synchronization of a One Identity Safeguard appliance marks the appliance as outstanding if the cluster that the appliance belongs to was swapped to another node in the preceding synchronization. A patch with the patch ID VPR#32031 is available for synchronization projects.	32031
If a domain with subdomains is connected to One Identity Safeguard, the `PrimaryAuthenticationProviderId` is determined incorrectly. A patch with the patch ID VPR#32423 is available for synchronization projects. IMPORTANT: Data in the One Identity Manager database goes missing when you apply this patch. To restore the data, start a full synchronization immediately after the automatic patches have been applied.	32423
Error loading objects that were not logged during synchronization if the **Continue on error** synchronization workflow is configured.	32099
Display names for `HREmployee_Active` are only shown in debug mode.	32130
Migration of the One Identity Manager database fails in large customer bases if the `HelperSAPUserInSAPRole` is updated.	32265
The system connection to SAP R/3 cannot be established if the synchronization user's password contains dollar ($) characters.	32298
Adding and deleting SAP user accounts does not trigger the recalculation task for the `SAPBWUserInSAPBWP` table.	32482, 32486
The option to login with user name and password is missing from the configuration for the system connection to SAP R/3 with SNC login. A patch with the patch ID VPR#32415 is available for synchronization projects.	32415
Parameters used to call a BAPI function to delete an SAP object are incorrectly populated.	32469
`SAPTitle.DistinguishedName` is not unique. A patch with the patch ID VPR#32584 is available for synchronization projects.	32584
Provisioning processes for different SAP user accounts are not processed simultaneously by the Job queue. This happens if the same reference user is assigned to the user accounts.	32318, 32638

Resolved issue	Issue ID
Error accessing the target system with the SCIM connector for One Identity Starling Connect.	31228
Patches for synchronization projects that use the SCIM connector are provided by the wrong One Identity Manager module.	32032
Error applying the VPR#29844 patch.	32044
If you use the SCIM connector to synchronize a GitHub system, queries from GitHub are rejected because the user agent is not included.	32535
Error testing the connection to the cloud application in the system connection wizards if there is no authentication endpoint given.	32627
Error defining a database view if a system connection is configured through the generic ADO.NET provider.	32251
The native database connector executes the configured processing method of a synchronization step only for the first object of the object class although several objects need to be processed. This happens if a pattern-based strategy is defined for the data operation.	32307
Error updating the schema from a CSV file if the file has not been declared in the system connection wizard.	32391
Error adding memberships in the `UNSAccountBInUNSGroupB` table in the target system browser although the object are within the scope.	32532
If the revision property does not contain a value (`NULL` or empty string), the wrong data type is saved in the `DPRRevisionStore` table.	32222
Problems connecting to Microsoft Exchange Server 2016 if using SSL.	32362
The `ThrottlingPolicy` property is not loaded for Microsoft Exchange mailboxes.	32533

Table 8: Identity and Access Governance

Resolved issue	Issue ID
The task `QER-K-OrgAutoChild` blocks the DBQueue.	31567
In certain circumstances, assignments on assignment forms are not saved.	32030
A potentially damaging SQL statement has been identified on different overview forms.	32170
Performance problems calculating system role assignment to business roles and organizations.	32546
The **Identity Lifecycle Customer** dynamic role has orphaned foreign keys if the **QER | ITShop** configuration parameter is not set.	31898

Resolved issue	Issue ID
Email notification about pending requests are sent to members of the chief approval team.	31996
If a system entitlement does not have a container, the **TO** approval procedure cannot determine an approver.	32162
If the number of approvers is given as **-1** (all employees found are approvers) in an approval step, the request is also presented for approval to the members of the chief approval team.	32172
Insufficient permissions for end users to delete or end a delegation.	32210
Escalation of an approval step does not take the **QER | ITShop | ReuseDecision** and the **QER | ITShop | AutoDecision** configuration parameters into account.	32318
New entries are created in the `PWOHelperPWO` table for requests with validity periods in the future that already have final approval.	32398
In certain circumstances, an employee can make an approval decision for a request that was questioned.	32465
If an additional approver was assigned to an approval step, the chief approval team's approval decision has no effect.	32467
The **Number of requestable products** statistic element shows the number of all the products in the IT Shop instead of just requestable products.	32503
Error removing a service category (`AccProductGroup` table) from the hierarchy.	32171
The `QER_ZITShopOrderAbort` procedure user the wrong cancellation method.	32522
If an approver makes approval decisions for several requests because they are delegated, the delegator is only informed the first time.	32526
In certain circumstances, despite the **QER | ITShop | DeleteClosed** configuration parameter being set, not all columns that are marked to be logged on deletion are logged.	32559
Increased occurrences of deadlock during parallel processing of requests (bulk requests).	32630
If E-Business Suite permissions assignments to user accounts are attested and automatic removal of permissions is configured, denied assignments are not deleted.	30375
The condition for viewing the `AttestationCase` table of the **VI_4_ALLUSER** permissions group does not allow closed attestation cases to be displayed if the currently logged in user was involved.	31365
If memberships of Azure Active Directory user accounts in groups	31955

Resolved issue	Issue ID
(ADDUserInGroup table) are attested and automatic withdrawal of system entitlements on attestation failure is configured, the wrong memberships are deleted if the group is an Office 365 group or an Exchange Online mail-enabled distribution group.	
If an approval step, for which a query was made, is escalated, the Hold status of the attestation case is not removed.	31991
If an attestation object is deleted during an attestation run, the entire attestation run is terminated.	32538
Automatic removal of permissions after attestation is not approved, does not taken into account if the assignment is marked for deletion.	32661
During synchronization of SAP authorization assignments to SAP groups, not all the objects are loaded. This means that rule violations are not found when SAP function compliance rules are checked.	32150
Error generating simple reports in CSV format.	32009, 32010, 32547
In certain reports about employees, the time period for assignments is not calculated correctly.	32389
Employees are shown on the **Subscribable report overview** form that do not subscribe to that report anymore.	32473

Table 9: IT Service Management

Resolved issue	Issue ID
The **VI_Asset_ServerHasShares_MasterData** form does not have a tab for custom columns.	32060
The **Help desk employee** option on an employee's master data form, is not displayed correctly if you swap between employees.	32587

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 29

Known issues

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

Table 10: 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
Headers in reports saved as CSV do not contain corresponding names.	24657
In certain circumstances, objects can be in an inconsistent state after simulation in Manager. If an object is changed or saved during simulation and the simulation is finished, the object remains in the final simulated state. It may not be possible to save other modifications to this object instance. Solution: Reload the object after completing simulation.	12753
Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation. Cause: The Configuration Wizard was started directly. Solution: Always use `autorun.exe` for installing One Identity Manager components. This ensures that you do not select any invalid modules.	25315
Schema extensions on a database view of type **View** (for example `Department`) with a foreign key relation to a base table column (for example `BaseTree`) or a database view of type **View** are not permitted.	27203
Error connecting through an application server or the API Server if the certificate's private key, used by the `VI.DB` to try and encrypt its session data, cannot be exported and the private key is therefore not available to the `VI.DB`. Solution: Mark the private key as exportable if exporting or importing the certificate.	27793
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.	29227
Error resolving events on a view that does not have a UID column as a primary key.	29535

Known Issue	Issue ID
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. The definition of a view that uses the `XObjectKey` as primary key, is not permitted and would result in more errors in a lot of other places. The consistency check **Table of type U or R with wrong PK definition** is provided for testing the schema.	
The default setting of `globallog.config` assumes that write access exists for `%localappdata%`. If an EXE does not have sufficient permissions, the log can be written to a directory that does have the access rights by changing the variable `logBaseDir` in the `globallog.config` or by introducing a special log configuration in the `*.exe.config` or the `Web.config` file.	30048
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.` Solution: Disable the option `DTC_SUPPORT = PER_DB`.	30972
If no date is given, the date 12/30/1899 is used internally. Take this into account when values are compared, for example, when used in reports. For detailed information about displaying dates and time, see the *One Identity Manager Configuration Guide*.	31322

Table 11: 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

Table 12: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use `Import-PSSession` internally.	23795
By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely. Solution: Make it possible to access the building block **HR_ENTRY_DATE** remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate` in the Synchronization Editor.	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
The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3. If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration. • Add a custom column to the table `SAPUser`. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required.	27359
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. 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.	27687
Error in IBM Notes connector (`Error getting revision of schema type ((Server))`). Probable cause: The IBM Notes environment was rebuilt or numerous entries have been made in the Domino Directory. Solution: Update the Domino Directory indexes manually in the IBM Notes environment.	27126
Error provisioning licenses in a central user administration's child system. Message: `No company is assigned`. Cause: No company name could be found for the user account. Solution: Ensure that either:	29253

Known Issue	Issue ID
• A company, which exists in the central system, is assigned to user account. - OR - • A company is assigned to the central system.	
Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will not come into effect until later. Cause: The function `BAPI_EMPLOYEE_GETDATA` is always executed with the current date. Therefore, changes are taken into account on a the exact day. Solution: To synchronize personnel data in advance that will not come into effect later, use a schema extension and load the data from the table `PA0001` directly.	29556
Error synchronizing an OpenDJ system, if a password begins with an open curly bracket. Cause: The LDAP server interprets a generated password of the form `{<abc>}<def>` as a hash value. However, the LDAP server does not allow hashed passwords to be passed. Solution: The LDAP server can be configured so that a hashed password of the form `{<algorithm>}hash` can be passed. • On the LDAP server: Allow already hashed passwords to be passed. • In the synchronization project: Only pass hashed passwords. Use the script properties for mapping schema properties that contain passwords. Create the password's hash value in the script.	29620
Target system synchronization does not show any information in the Manager web application. Workaround: Use Manager to run the target system synchronization.	30271
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**: `400: Bad Request -- 60639: A valid account must be identified in the request.` The request is denied in One Identity Manager and the error in the request is displayed as the reason.	796028, 30963
Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled. Cause: The SharePoint connector loads all object properties into cache by default.	31017

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. 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.	31904
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. 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> • In the new section: <SAP.Middleware.Connector> <GeneralSettings anyDateTimeValueAllowed="true" /> </SAP.Middleware.Connector>	32149

Table 13: 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. Solution: Parent IT Shop nodes of shelves and shops cannot be changed once they have been saved. ***To move a product in a shelf to another shop*** • 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. Once you have moved all the products, you can delete the shelf.	31413
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 14: 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
	29607
Memberships in Active Directory groups of type **Universal** in a subdomain are not removed from the target system if one of the following Windows updates is installed: • Windows Server 2016: KB4462928 • Windows Server 2012 R2: KB4462926, KB4462921 • Windows Server 2008 R2: KB4462926 We do not know whether other Windows updates also cause this error. The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory groups during provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem.	30575
In certain circumstances, the wrong language is used in the Stimulsoft controls in the Report Editor.	31155

In the Manager web application, following errors can occur under Windows Server 2008 R2:
`System.Security.Cryptography.CryptographicException: Object was not found.`
`at System.Security.Cryptography.NCryptNative.CreatePersistedKey (SafeNCryptProviderHandle provider, String algorithm, String name, CngKeyCreationOptions options)`
Workaround:
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.
	31995

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

Schema changes

The following provides an overview of schema changes in One Identity Manager version 8.1.1 up to version 8.1.2.

Configuration Module

- New table QBMDBQueuePond as buffer for DBQueue Processor tasks.
- New column QBMBufferTransfer.SortOrder as sort order for installing schema changes using the new method for updating the One Identity Manager database faster.

Target System Base Module

- Shortened the column UNSAccount.AccountName to nvarchar(400).

Azure Active Directory Module

- Shortened the column AADUser.UserPrincipalName to nvarchar(400).

Privileged Account Governance Module

- New columns PAGUser.UID_PAGAuthProviderPrimary and PAGUser.UID_ PAGAuthProviderSecond for mapping authentication providers for PAM user accounts.
- New column PAGUser.UID_PAGIdentityProvider for mapping identity provider for PAM user accounts.
- The columns PAGUser.UID_PAGIdentityProviderPrimary and PAGUser.UID_ PAGIdentityProviderSecond have been deleted.

Cloud Systems Management Module

- Columns CSMUser.AccountName and CSMGroup.cn extended to nvarchar(256).

Universal Cloud Interface Module

- Columns UCIUser.AccountName and UCIGroup.cn extended to nvarchar(256).

Identity Management Base Module

- Column DynamicGroup.DisplayName extended to nvarchar(256).

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 8.1.1 to version 8.1.2. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 57.

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 29.

Table 15: Overview of synchronization templates and patches

Module	Synchronization template	Type of modification
Azure Active Directory Module	Azure Active Directory synchronization	none
Active Directory Module	Active Directory synchronization	changed
Active Roles Module	Synchronize Active Directory domain via Active Roles	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)	changed

Module	Synchronization template	Type of modification
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)	changed
Privileged Account Governance Module	One Identity Safeguard synchronization	changed
SAP R/3 User Management Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	changed
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	changed
SAP R/3 Compliance Add-on Module	SAP R/3 authorization objects	changed
SAP R/3 Structural Profiles Add-on Module	SAP R/3 HCM authentication objects	changed
	SAP R/3 HCM employee objects	changed
SharePoint Module	SharePoint synchronization	none
SharePoint Online Module	SharePoint Online synchronization	none
Universal Cloud Interface Module	SCIM Connect via One Identity Starling Connect	none
	SCIM synchronization	none
Unix Based Target Systems Module	Unix Account Management	none
	AIX Account Management	none

Patches for synchronization projects

The following is a list of all patches provided for synchronization projects in One Identity Manager 8.1.2. 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 57.

Table 16: 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 17: 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 18: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#32667	Deletes the alternative objects mapping rules from the **oRA-Requestgroup** mapping	Deletes the object mapping rule **Identifier <-> REQUEST_GROUP_ID** from the **oRA-Requestgroup** mapping. This patch is applied automatically when One Identity Manager is updated.	32667
VPR#30464_1	Rollback of patch VPR#30464	Rolls back the changes from Patch VPR#30464. Support for Oracle Database Editions is resolved in the Oracle E-Business Suite. This patch is applied automatically when One Identity Manager is updated.	30464

Table 19: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#32031	Expose virtual appliance ID directly	Sets a virtual appliance ID in the connector schema and applies it to the	32031

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

Table 20: 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 21: 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 22: 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 23: 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
VPR#31792	Object filter correction	Corrects object filters. This patch is applied automatically when One Identity Manager is updated.	31792

Table 24: 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 25: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#30269	Prevents errors	Changes the schema properties `vrtModBy`,	30269

Patch ID	Patch	Description	Issue ID
	when loading single objects due to identical display names	`vrtAcceptMessagesFrom`, `vrtGrantSendOnBehalfOfTo`, `vrtRejectMessagesFrom` and all property mapping rules for these schema properties.	
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 26: 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 updated.	31735
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 27: 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 28: 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)** This patch is applied automatically when One Identity Manager is updated.	31568
VPR#31568B	Replaces **Appliance serial** as appliance identifier with a custom identifier (part 2)	Replaces **Appliance serial** as the unique identifier of the base object with a custom identifier and applies this change to the synchronization configuration. Dependent upon patch **Replaces Appliance serial as appliance identifier with a custom identifier (part 1)** This patch is applied automatically when One Identity Manager is updated.	31568
VPR#31569	One Identity Safeguard cluster access improvements	Adds connection parameters and variables for connecting One Identity Safeguard clusters. This patch is applied automatically when One Identity Manager is updated. If you use One Identity Safeguard clusters, run the system connection wizard after applying the patch, to determine the cluster's appliances.	31569
VPR#31664A	AccessRequestPolicy model changes	An access request policy can have multiple directory accounts for session	31664

Patch ID	Patch	Description	Issue ID
	for session access (part 1)	access. Prerequisite for patch **AccessRequestPolicy model changes for session access (part 2)**. This patch is applied automatically when One Identity Manager is updated.	
VPR#31664B	AccessRequestPolicy model changes for session access (part 2)	An access request policy can have multiple directory accounts for session access. Dependent on patch **AccessRequestPolicy model changes for session access (part 1)**. This patch is applied automatically when One Identity Manager is updated.	31664
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 29: 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 30: 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 31: 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 32: 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 33: Patches for Azure Active Directory

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

Table 34: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#29087	Add the schema property `mS-DS-ConsistencyGuid`	Adds the schema property `mS-DS-ConsistencyGuid` in the `User` and `InetOrgPerson` maps.	29087
VPR#29306	Schema class `ADSSite (all)` (part 1) correction	Changes the foreign key for `ADSSite` from `ADSDomain` to `ADSFroest`. Prerequisite for patch **Schema class ADSSite (all) (part 2) correction**. This patch is applied 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 35: 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 36: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#28962_EBS	Change date conversion in script properties	A language independent format is used for converting date values in script properties. This patch is applied automatically when One Identity Manager is updated.	28962
VPR#29265	Extended processing methods in the synchronization step HR PersonManager	Extended the synchronization configuration EBS_Person_RemoveManager in the synchronization step HR PersonManager. This patch is applied 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 37: 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 38: 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 39: Patches for G Suite

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

Table 40: Patches for LDAP

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

Table 41: Patches for IBM Notes

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

Table 42: 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	30941

Patch ID	Patch	Description	Issue ID
		the provisioning workflow. This patch is applied automatically when One Identity Manager is updated.	
	Milestone 8.1	Milestone for the context **SAP R/3**.	

Table 43: 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 when One Identity Manager is updated.	29265
	Milestone 8.1	Milestone for the context **SAP R/3 structural profile add-on**.	

Table 44: 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 45: 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 46: Patches for SharePoint

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

Table 47: 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 48: 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 49: 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 50: Patches for Unix

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

Table 51: Patches for the One Identity Manager connector

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

Table 52: 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_ADSAccountInADSGroup
  - 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 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 template 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 • Note the requirements from Microsoft for the SQL Server version installed. UNIX and Linux operating systems • Note the minimum requirements given by the operating system manufacturer for SQL Server databases.
Software	Following versions are supported: • 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 • 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: • 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.
Additional software	Windows operating system • Microsoft .NET Framework Version 4.7.2 or later NOTE: Take the target system manufacturer's recommendations for connecting the target system into account. Linux operating system • Mono 5.14 or later

Minimum requirements for clients

Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	1 GB
Operating system	Windows operating system • Windows 10 (32-bit or 64-bit) with version 1511 or later • Windows 8.1 (32-bit or 64-bit) with the current service pack • Windows 7 (32-bit or non-Itanium based 64-bit) with the current service pack
Additional software	• Microsoft .NET Framework Version 4.7.2 or later
Supported browsers	• Internet Explorer 11 or later • Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimum requirements for the Web Server

Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM

Hard drive storage	40 GB
Operating system	Windows operating system • Windows Server 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 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 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)

Supported data systems

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

Table 53: 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.
Gerneric 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	• Microsoft Exchange 2010 Service Pack 3 or later • Microsoft Exchange 2013 with cumulative update 23

Connector	Supported data systems
	• Microsoft Exchange 2016 • Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange hybrid environments
SharePoint connector	• SharePoint 2010 • SharePoint 2013 • SharePoint 2016 • SharePoint 2019
SAP R/3 connector	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2 and 7.50 • SAP ECC 5.0 and 6.0 • SAP S/4HANA On-Premise-Edition
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the Authentication Services specifications.
IBM Notes connector	• Lotus Domino Server version 8.0 up to Lotus Domino Server version 10.0 • In the client version, IBM Notes client 8.5.3 and 10.0 are supported.
Native database connector	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA
Mainframe connector	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 6.9, 7.0, 7.2, 7.3.1

Connector	Supported data systems
Azure Active Directory connector	• Microsoft Azure Active Directory 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.
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0.
Exchange Online connector	• Microsoft Exchange Online
G Suite connector	• G Suite
Oracle E-Business Suite connector	• Oracle E-Business Suite System versions 12.1 and 12.2
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard versions 2.5, 2.6, 2.7, 2.8, 2.9, 2.10 and 2.11

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 8.1.2 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 52.

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 8.1.2. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
  - Automatic software updating of version 7.0 to version 8.1.2 only works smoothly if the service pack 7.0.3 is installed. In addition, the files `VI.Update.dll` and `JobService.dll` must be installed.

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

    To distribute the file, use the Software Loader.

    Future service packs of 7.0 versions will already contain the changes to these files, and therefore, must not distributed separately.
  - Automatic software updating of version 7.1 to version 8.1.2 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. Ensure that the user that going to execute the installation or update of the One Identity Manager database, owns the **dbcreator** SQL Server server role.
- During the update of a One Identity Manager database version 7.0, 7.1 or 8.0 to version 8.1.2, 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 8.1.2 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 8.1.2, 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 8.1.2

IMPORTANT: Note the Advice for updating One Identity Manager on page 52.

To update an existing One Identity Manager installation to version 8.1.2

1. Run all the consistency checks in the Designer in **Database** section.
   a. Start the Consistency Editor in the Designer using the **Database | Check data consistency** menu item.
   b. In the **Test options** dialog, click  .

c. Under the **Database** node, enable all the tests and click **OK**.

d. Start the check by selecting the **Consistency check | Run** menu item.

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

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

   a. Execute the program `autorun.exe` from the root directory on the One Identity Manager installation medium.

   b. Change to the **Installation** tab. Select the Edition you have installed.

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

   c. Click **Install**.

      This starts the installation wizard.

   d. Follow the installation instructions.

      IMPORTANT: 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 8.1.2, 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 8.1.2, 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.

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 8.1.2

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

   NOTE: Some patches are applied automatically. A process that migrates all existing synchronization project is queued in the Job queue to do this. To execute

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

- Check whether the process `DPR_Migrate_Shell` 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 57.

To update an application server to version 8.1.2

- 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 8.1.2

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

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

To update an API Server to version 8.1.2

- 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 8.1.2

- (As from version 8.1.x) After updating the API Server, compile the HTML application **Operations Support Portal**. For more information, 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 information, see the *One Identity Manager Installation Guide*.

To update the Manager web application to version 8.1.2

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

See also:

- Modified synchronization templates on page 28
- Patches for synchronization projects on page 29

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 2019.0001.0021.0200 for all modules and the application version 8.1 2019-01-21-229 indicate that this version is installed.

Additional resources

Additional information is available from the following:

- One Identity Manager support
- One Identity Manager online documentation
- Identity and Access Management community
- One Identity Manager training portal

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

For sales 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

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.