One Identity Manager 8.1.3

Release Notes

June 2020

These release notes provide information about the One Identity Manager release, version 8.1.3. You will find all the modifications since One Identity Manager version 8.1.2 listed here.

One Identity Manager 8.1.3 is a patch release with new functionality and better behavior. See New features on page 2 and Enhancements on page 3.

If you are updating a One Identity Manager version prior to One Identity Manager 8.1.2, 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 8.1.3

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 8.1.3:

Basic functionality

- Improved support for encrypting a database. If you are installing a new database, you can encrypt it immediately with the Configuration Wizard. To do this, the Configuration Wizard opens a new page called **Database encryption**.
- To support troubleshooting in OAuth 2.0/OpenID Connect authentication you can log personal login data, such as information about tokens or issuers. The log is written to the object log file (`<appName>_object.log`) of the respective One Identity Manager component. The **QBM | DebugMode | OAuth2 | LogPersonalInfoOnException** configuration parameter defines whether the login data is recorded.
- Running of all automatic schedules can be temporarily stopped. This behavior is controlled by the new **QBM | Schedules** configuration parameter. If the configuration parameter is set, schedules are run automatically. If the configuration parameter is not set, schedules are not run automatically. However, you can start the schedules manually.

Web applications

- In the Web Portal, you can now use heatmaps to show how many requests have been generated for each department, cost center, location or business role. This allows "hot spots" to be identified, meaning places in the organization that generate an unusually high number of access requests. This helps determine common characteristics of such access requests to aid decisions for investments in policy and role management. In the Web Portal, open the heatmaps on the home page's **Request | Explore** tile.
- In the Web Portal, it is now possible to control how table columns are sorted by using the keyboard.

Target system connection

- One Identity Safeguard version 6.0 is supported.
- Simplified system connection wizards for Active Roles.

  On the **Target server** page, the system connection wizard now tries to find the service entries under `CN=Enterprise Directory Manager,CN=Aelita,CN=System,<Domain DN>` using the current login credentials. If the entries are found, their DNS names are provided in a menu. If no entries are found, the user can enter the target server manually.
- Support for dynamic Azure Active Directory groups.
- Support for dynamic Office 365 groups.
- HCL Domino Server Version 11 and HCL Notes Client Version 11.0.1 are supported.

See also:

- Enhancements on page 3
- Resolved issues on page 7
- Schema changes on page 24
- Patches for synchronization projects on page 26

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.1.3.

Table 1: General

Enhancement	Issue ID
The `FileComponent` process component support path lengths of more than 260 characters.	30846

Enhancement	Issue ID
New parameters of the `ScriptComponent` process component are available for the `CSVExport` and `CSVExportSingle` process tasks. • `ValueMaskChar`: Character for masking values. If the parameter exists, the character is automatically added at both ends of each value and every time the same character appears within the value, it is doubled. • `Culture`: Language to use for formatting the value. • `ConvertUtcTimes`: Specifies whether UTC times are converted to local times. • `TimeZone`: For converting to the timezone to use. Only used if the `ConvertUtcTimes` is set. If the parameter is not set, the Job server's local timezone is used. • `ParameterSet`: UID of the parameter set to use. If the parameter is set, the parameter set is loaded and the parameters are made available to the query as `Query` parameters.	32410, 32939, 33039
More tolerant handling of temporary errors in the schema update.	32867
Improved functionality for the Launchpad. • You can create tasks that can be run straight from the Launchpad. • Menu items in the Manager can be opened straight from the Launchpad.	32909, 33007, 33037
You can now enter more than one value in the **TargetSystem | LDAP | Authentication | RootDN** configuration parameter using a pipe (|) delimited list. For example, **DC=Root1,DC=com|DC=Root2,DC=de**. The LDAP authentication modules check authentication against each of the root domains. Verification of login credentials with an LDAP authentication module has been optimized. LDAP user accounts that are not assigned to an employee, are not taken into account anymore. The domains entered in the user accounts are used for verification (`LDAPAccount.UID_LDAPDomain`).	33112
Improved error logging in the application server.	33115

Table 2: General web applications

Enhancement	Issue ID
In the Web Portal, keyboard shortcuts for buttons are now displayed in full (for example, **[Alt-C]**).	31882
In Web Portal, the version number is shortened (for example 8.1).	32966
In the Web Portal, the option to change the priority of all products when you edit the shopping cart has been renamed.	33057

Enhancement	Issue ID
Improved performance when checking the shopping cart in the Web Portal.	32765
Improved security generating reports in the Web Portal.	32869
Improved support for HTTP header authentication if the connection goes through an application server.	32794
Improved accessibility in the Web Portal when displaying tiles in high contrast mode.	203449
The `Microsoft.OData` library has been updated to the newest version.	235855
If API resources (Typescript client and Swagger JSON) are not required for compiling the API, The API resources can now be generated in the `DbCompiler.exe` file using the `DoNotBuildResources` parameter. For example, this might be necessary if problems occurs during compiling.	233720
The information saved in the sessions cookies of an API Server session now expire if the customer restarts the browser.	225773

Table 3: Target system connection

Enhancement	Issue ID
Improved error messaging for load operations in the synchronization log.	33006
The SCIM connector now uses the service provider's default value to find the maximum number of objects per page. The connector does not send values anymore.	32684
Improved performance provisioning G Suite user accounts.	32884
You can configure which user data is transferred to a different user account before G Suite user accounts are deleted.	33104
Improved documentation of permissions required for integrating One Identity Manager as an application in Azure Active Directory.	32820
The filter for the `HRPerson_0709_IDEXT` schema class was changed from a string to an integer comparison. A patch with the patch ID VPR#32899 is available for synchronization projects.	32899
Improved messages for the SCIM connector in the synchronization log.	32689, 32690
The SCIM connector detects whether the service provider requires URLs with a closing slash.	32843
The recommendations from Microsoft about avoiding throttling during SharePoint Online synchronization have been implemented.	32929

Enhancement	Issue ID
The Active Directory connector can use the One Identity Manager Service's user account to log in on the target system. To do this, leave the login credentials on the project wizard's **Login** page empty.	32693
The Microsoft Exchange connector can use the One Identity Manager Service's user account to log in on the target system. To do this, in the project wizard enable the **Use account of One Identity Manager Service** option on the **Enter connection credentials** page. A patch with the patch ID VPR#32703 is available for synchronization projects.	32703
In the project wizard for connecting cloud applications in the Universal Cloud Interface, the cloud application menu has been made larger.	32955
In an SAP schema extension file, you can provide a time offset for the revision counter (`AddRevisionTimeOffset` attribute) in the schema type definition. You can use this attribute if the revision counter only contains a change date but no timestamp. This allows objects that were changed after the previous synchronization run but on the same day, to be included in the next synchronization run.	32739
Adjustments required to the Exchange Online connector due to Microsoft turning off functionality in the cloud.	32403
You can configure whether the database to be connected takes case sensitivity into account for the generic ADO.NET provider.	33081
Improved performance calculating user account assignments to groups in custom target systems (`UNSAccountBInUNSGroupB` table).	33070

Table 4: Identity and Access Governance

Enhancement	Issue ID
Improved performance creating and by approval of attestation cases.	32940
Improved indexing of the `PersonHasObject` and `BaseTreeHasObject` tables.	32771
In the Manager, on the overview forms for application roles, departments, cost centers, location and business roles, you can now see which approval workflows they are used in.	32745
Improved support for peer group analysis for attestation.	32328

See also:

- Schema changes on page 24
- Patches for synchronization projects on page 26

Resolved issues

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

Table 5: General known issues

Resolved issue	Issue ID
Blocked slots are reset too frequently.	32585
Error calculating time periods for memberships in reports with historical data.	32726
Transaction scope of the DBQueue Processor's `HDB-K-ProcessGroup` task is too big.	32761
Processes are sporadically not generated from schedules.	32742
Input of dates in reports does not support every date format.	32775
When a report is translated, the description is not translated.	32875
The `RPS_ParseReportDefinitionXML` script takes disabled columns into account when calculating the row definition.	33025
The **Table with XOrigin (XIsInEffect) without update handling** consistency check does not take automatically generated triggers into account.	32902
The result of a SQL query in the Object Browser cannot be marked with **Ctrl + A** anymore.	32942
If you change the foreign key on an object in the Object Browser and use the **Discard** button to discard the changes, the foreign key is not reverted.	32387
If the time difference to UTC for a timezone changes, the mean time difference to UTC for the states in this timezone is not updated.	32973
In certain circumstances, the following error occurs when the Crypto Configuration encrypts long strings: `String or binary data would be truncated.`	32161
Some Austrian states are not shown in the national language.	32676
Deferred DBQueue Processor tasks are included in the performance calculation.	32747
Bad performance running DBQueue Processor tasks with 2 parameters.	32906
Bad performance when, in the Job queue, there are a lot of similar processes for different queues.	32813
Incorrect handling of custom triggers during database compilation after changes to the schema.	32793, 32962
Export definitions for data export are not saved in the user configuration and are therefore not available after the Manager has been restarted.	32887

Resolved issue	Issue ID
In Launchpad, if you search for an item and right-click on the result, in the context menu **Remove from favorites** is shown instead of **Add to favorites**.	32828
In a One Identity Manager database with version 7.x, the `\SDK\SQLSamples\Files\MSSQL2K\30374.sql` script does not detect an empty `ADSSite.UID_ADSDomain`.	32891
For initial migration with the provided database, the user requires the SQL Server **dbcreator** server role.	33001
In certain circumstances, an object is saved more than once after running a template. The following message is displayed: `<object> was changed by another user`.	33063
Error automatically updating software after updating a One Identity Manager database from version 8.1 if the database is part of an AlwaysOn Availability Group.	33068
In certain circumstances, while using the LDAP authentication module, the `Login failed` or `VI.Base.ViException: Wrong user name or password` error occurs even though the correct login credentials were used.	33107
Changes to `DialogTable.isMNTable` and `DialogTable.IsMAllTable` do not generate a recalculation task for `Watch*` trigger.	33109

Table 6: General web applications

Resolved issue	Issue ID
In certain circumstances in the Web Portal, the scroll bars are missing in the product's detailed view and, therefore, not all the data is visible.	32511
In certain circumstances in the Web Portal, the **View Settings** menu is shown twice in the search results after a search.	32598
In the Web Portal date columns, if you filter with **Before**, objects that do not have a value in the corresponding field are, incorrectly, displayed as well.	32686
In certain circumstances in the Web Portal, pending attestation are not displayed.	32755
In the Web Portal, an error occurs if an empty grouped table is exported as a PDF.	32773
In the Web Portal, values are being validated in fields although the input is not yet complete.	32786
Under Safari, permitting browser notifications in the Web Portal causes an error.	32787
In the Web Portal, an error occurs if a request for a product is displayed and it	32837

Resolved issue	Issue ID
is not assigned to an IT Shop.	
In the Web Portal, if a direct assignment of an SAP role to an SAP user account is removed, the associated entry in `SAPUserInSAPRole` is not deleted.	32842
If several products in the shopping cart are tested for requestability and there is a conflict, all products are marked the same. To make it easier to differentiate, in the **VI_ITShop_ShoppingCart** Web Designer component, a new **Warning** value has been introduced for the **CheckStatus** property in the **ShoppingCart** collection. Customized components that show this property must also take this new value into account.	32863
An error occurs when an approver in the Web Portal adds an item to another employee's request and sends the request.	32880
In the Web Portal, requests to be approved can be selected in a list. In certain circumstances, the selection goes missing when you switch to the another page of the list.	32904
In the Web Portal, an error occurs if you use the function to split a role that you are responsible for.	32913
In the Web Portal, on the **Pending attestations** page, an error occurs when you click the **Business roles** tile.	32920
In the Web Portal, if you download a file with Internet Explorer 11 whose name contains non-ASCII characters, an incorrect file name is suggested for the file.	32921
When a request is being approved in the Web Portal, it is possible to set the end of the validity period before the beginning of the validity period.	32928
In the Web Portal, if a new child group is added, it is not shown in the list of child groups until the next login.	32981
In the Web Portal, deleting objects causes performance problems as well as problems with the search function.	32987
In the Web Portal, if you filter delegations by recipient and the number of results is more than 1000, only the first 1000 are shown.	33019
If an error alert is displayed in the Web Portal and you try to close it using the **Escape** key, the underlying dialog is closed instead of just the error alert.	33020
In the Web Portal, there is no information about what date format is expected.	33054
In the Web Portal, if an error occurs validating date input, the focus is not automatically set in the corresponding field.	33055
Logging in to the Web Portal using OAuth 2.0/OpenID Connect does not work	32879

Resolved issue	Issue ID
flawlessly.	
Bad performance of the pre-defined `Webportal.VI_ITShop_ProductSelection.AccProductStatusForPerson` SQL statement.	32767
In Web Designer, if you add a column of `XdateInserted` or `XdateUpdated` type to a table, the filter function for the column does not work in the Web Portal.	32709
The Web Designer's `GetDataState` function does not work and returns a value of **false** even if columns have changed.	32790
In certain circumstances, memory usage increases whilst working with the Web Designer.	32900
In the Web Designer's navigation, none of the existing custom components are listed under **Components**.	33040
In the Web Designer, if you open a context menu in a tree view with a right click, an error occurs.	33085
If you deactivate the configuration key **VI_RSTS_UseRedirect** in the Web Designer, you can no longer log in to the Web Portal using RSTS.	33148
Incorrect translations in the Web Designer Configuration Editor for the OAuth 2.0/OpenID Connect configuration.	32806
The following error occurs running the API server: `The CancellationTokenSource has been disposed.`	32914
Logging in to the Manager web application fails if TLS 1.0 or TLS 1.1 is disabled on the web server.	32854

Table 7: Target system connection

Resolved issue	Issue ID
The `IsSecret` and `IsSystemVariable` properties of the `DefaultUserPassword` variable are not all correctly set in the synchronization project. Patches with patch IDs VPR#32781_SCIM, VPR#32781_EBS, VPR#32781_NDO are available for synchronization projects.	32781
Error applying a patch to a synchronization project after migrating to One Identity Manager version 8.1.2.	32785
Error loading an object if an object class' unique key is defined as a column group and the value of one of the columns is **NULL**.	32817
Provisioning a single group membership takes too long.	33074
If synchronization projects are updated from the command line and the `Patches=AllFixes` parameter is set at the time, the milestones are not imple-	33123

Resolved issue	Issue ID
mented.	
If an Active Directory object that already has the `SAMAccountName` exists in another container in Active Directory, an error occurs.	32504
The `Value of parameter 'distinguishedName' cannot be converted to an ADSI path` error message does not include the DN passed down.	32849
Error during synchronization if accessing special properties of Active Directory objects using a `DirectoryEntry` object's `extension` method.	32873
Active Directory account policies that are assigned through Active Directory groups are not taken into account in Active Directory user accounts.	32803
In the Manager, the Active Directory **Change master data** form does not show changes to the **Dial-up permitted** property in Active Directory user accounts (`ADSAccount.AllowDialIn`).	32889
Wrong reference scope for Active Directory locations. A patch with the patch ID VPR#32965 is available for synchronization projects.	32965
In certain circumstances, Active Directory synchronization fails with the error: `Value cannot be null`.	33022
An error occurs when reading and writing Active Directory object properties that are read or written using an extension method.	33120
Error during provisioning when restoring a deleted Active Directory object with activated Active Directory recycle bin feature.	33125
The Active Roles connector does not support the function level for Windows Server 2016 domains. A patch with the patch ID VPR#32844 is available for synchronization projects.	32844
The `edsaWTSUserConfigInheritInitialProgram` property in the `User` mapping is negated. This behavior is no longer required. A patch with the patch ID VPR#32871 is available for synchronization projects.	32871
Error serializing complex properties from schema extensions in synchronization projects with the SCIM connector.	32696
The SCIM connector uses the wrong media type for `POST` queries in the HTTP header. The data is swapped around.	32712
The `User.address~primary` schema property is set to **True** even if no address data is given. A patch with the patch ID VPR#32754 is available for synchronization projects.	32754
Error loading the object list during a cloud application synchronization if the	32757

Resolved issue	Issue ID
object list contains an object without a creation date .	
The provisioning process for a cloud application's user accounts returns the wrong data for loading the objects.	32780
In synchronization projects that were created with the One Identity Starling Connect project template, mapping telephone numbers does not work when provisioning changes.	32831
Error provisioning in a cloud application if there is a read-only virtual schema property in the object matching rule.	32841
Error provisioning group memberships if the SCIM connector uses `PATCH` queries.	32846
Provisioning of deleted group memberships does not work under certain conditions.	32853
Changes to values of multi-valued schema properties are not correctly mapped in `PUT` queries.	32901
Checking for the existence of target system objects fails if there are several mappings.	32908
During synchronization, an invalid entitlement assignment is not re-enabled if it exists in Oracle E-Business Suite as a valid assignment. `EBSUserInResp.XOrigin` retains the value **16**.	33024
Error provisioning Notes user accounts if the user account's certificate has been changed.	32705
After updating Notes group memberships, the `Summary` and `Names` options are not set on the `Members` schema property anymore.	32766
The process for locking Notes user accounts does not work correctly.	32947
If SAP user accounts marked for deletion are reset, the associated `SAPUserInSAPRole` entries remain marked for deletion and are not reset.	32727
The `IsSecret` and `IsSystemVariable` properties of the `TempUserPassword` variable are not all correctly set in the synchronization project. A patch with the patch ID VPR#32781_SAP is available for synchronization projects.	32781
If a One Identity Manager user account is renamed in SAP, not all existing assignments are transferred to the new user account by provisioning, only the last one.	32807
Assigning or removing a direct membership in `SAPUserInSAPRole` that is already inherited generates the provisioning process.	32951

Resolved issue	Issue ID
Synchronizing SAP authorizations does not load all authorization object assignments to SAP transactions (`SAPTransactionHasSAPAuthObject`).	33044
The reference scope for the `SAPLicence` table is so restrictive that in the SAP R/3 environment existing license assignments in the `SAPUserHasLicence` table cannot be added.	33071
On the SAP user accounts' overview form, the assigned composite profiles from a CUA's child system are not displayed.	33094
If single object synchronization is run several times sequentially on an Exchange Online mailbox, the value for `XMarkedForDeletion` swaps back and forth between **0** and **2**. A patch with the patch ID VPR#32768 is available for synchronization projects.	32768
Error provisioning G Suite user accounts in One Identity Manager version 8.1.2.	33073
Error loading single objects with Windows PowerShell if the parameter `Identity` is used.	32818
Performance problems deleting memberships during single object synchronization.	32673
In the Manager, custom columns of `Datetime` type are not displayed with the desired alternative column identifier for custom target systems.	32702
On the form for defining search criteria for employee assignment, employees' display names are not correctly formatted.	32876
The following error occurs when the `UNSAccountB.CN` template is run: `Entry point was not found`.	32825
In the Manager, on the **Change master data** form for custom groups, the category cannot be selected if it does not have a container.	31592
If an Exchange Online synchronization project is opened in an encrypted database in the Synchronization Editor, it is not possible to identify which password belongs to which user.	33118

Table 8: Identity and Access Governance

Resolved issue	Issue ID
Notifications from questions about an attestation case are sent to the wrong employee.	32809
Error adding attestation cases.	32988
Error automatically removing E-Business Suite entitlement assignments after	32961

Resolved issue	Issue ID
attestation has been denied.	
The GenProcID in requests is emptied too quickly if an approved request's validity period is in the future.	32720
Automatic approval decisions caused by the **QER | ITShop | DecisionOnInsert** or **QER | ITShop | AutoDecision** configuration parameter settings are also decided for the chief approval team.	32743
The consistency check's repair script **Requested products that are not assigned** generates missing entries in the `PersonInITShopOrg` table with the wrong value for `XOrigin`.	32827
Under certain circumstances, when determining a request's approver, a fallback approver is not found although there is no regular approver.	32872
If in the second approval step of an approval workflow, the approval method EX is used and approval of the first approval step was decided automatically, the process for external approval is not triggered.	32886
If the `QER-K-ShoppingRackMakeDecisionEX` task is returned to the DBQueue, in One Identity Manager 8.1.2 external approval is triggered again. Therefore the process for external approval is started twice.	32898
The display name for the requested product is not displayed in requests (`PersonWantsOrg.DisplayOrg`) if the product exists on more than one shelf.	32969
Shops cannot be separated from shopping centers that are assigned a shopping center template.	32993
Error importing SAP functions if the One Identity Manager database is connected through an application server.	32678
If, in the permissions editor for SAP functions, one of the **Add by** tasks is run and One Identity Manager is running over an application server, the Manager freezes.	32789
Bad performance in the DBQueue Processor `SAC-K-ProfileHasTCDInFID` task.	32805
The **Replace** method is not available for requests with `Renewal` status.	33029
Error removing shops from shopping centers.	32999
In the Manager, the **Additional information** column (`PersonWantsOrg.AdditionalData`) is missing from the **Request details** form.	33102

Table 9: IT Service Management

Resolved issue	Issue ID
In the Manager, diverse master data are missing from the PC and server	32922

Resolved issue	Issue ID
master data forms.	
Error adding a help desk call: `Error executing script 'VI_AE_GetAttachmentPath'.`	33019

See also:

- Schema changes on page 24
- Patches for synchronization projects on page 26

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	27203

Known Issue	Issue ID
database view of type **View** are not permitted.	
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. 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.	29535
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
The following error occurred installing the database under SQL Server 2019: `QBM_PDBQueueProcess_Main unlimited is only allowed as an agent job` Solution:	32814

Known Issue	Issue ID
• The cumulative update 2 for SQL Server 2019 is not supported. For more information, see https://support.oneidentity.com/KB/315001.	

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
It is not possible to use the Web Designer to place a link in the header of the Web Portal next to the company name/logo.	32830
In the Web Portal, it is possible to subscribe to a report without selecting a schedule. Workaround: • Create an extension to the respective form that displays a text message under the menu explaining the problem. • Add a default schedule to the subscribable report. • In the Web Designer, change the **Filter for subscribable reports** configuration key (**VI_Reporting_Subscription_Filter-RPSSubscription**) and set the schedule's **Minimum character count** value (`UID_DialogSchedule`) to **1**.	32938

Table 12: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use `Import-`	23795

Known Issue	Issue ID
PSSession internally.	
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: • A company, which exists in the central system, is assigned to user account.	29253

Known Issue	Issue ID
- 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. Solution: • Correct the error in the target system.	31017

Known Issue	Issue ID
- 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>`
• A new section:
`<SAP.Middleware.Connector>`
`<GeneralSettings anyDateTimeValueAllowed="true" />`
`</SAP.Middleware.Connector>`
	32149

There are no error messages in the file that is generated in the `PowershellComponentNet4` process component, in `OutputFile` parameter. Cause: No messages are collected in the file (parameter `OutputFile`). The file serves as an export file for objects returned in the pipeline.	32945

Known Issue	Issue ID
Solution: Messages in the script can be outputted using the *> operator to a file specified in the script. Example: `Write-Warning "I am a message" *> "messages.txt"` Furthermore, messages that are generated using `Write-Warning` are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an `Exception`. This message then appears in the One Identity Manager Service's log file.	

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	24784

Known Issue	Issue ID
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.	
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, 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
	31995

Known Issue	Issue ID
application and then the **Advanced Settings** context menu item. 2. On the **Process Model** panel, set the option **Load User Profile** to **True**. For more information, see https://support.microsoft.com/en-us/help/4014602.	
When connecting an external web service using the web service integration wizard, the web service supplies the data in a WSDL file. This data is converted into Visual Basic .NET code with the Microsoft WSDL tools. If, in code generated in this way, default data types are overwritten (for example, if the `boolean` data type is redefined), it can lead to various problems in One Identity Manager.	31998

In certain Active Directory/Microsoft Exchange topologies, the `Set-Mailbox` Cmdlet fails with the following error:
`Error on proxy command 'Set-Mailbox...'`
`The operation couldn't be performed because object '...' couldn't be found on '...'.`
For more information, see https://support.microsoft.com/en-us/help/4295103.
Possible workarounds:
• Connect to the Microsoft Exchange server that the user mailbox is on. Use a custom process to do this. Use the `OverrideVariables` parameter (`ProjectorComponent` process component) to overwrite the server (`CP_ExchangeServerFqdn` variable).
• Because this problem only occurs with a few schema properties, you should consider protecting these schema properties in the synchronization project against write operations. You can set the schema properties in a custom process using the `PowershellCompomentNet4` process component through a user-defined Windows PowerShell call.
	33026

Schema changes

The following provides an overview of schema changes in One Identity Manager version 8.1.2 up to version 8.1.3.

Configuration Module

- New column `QBMLaunchAction.UID_QBMClrType` for use with special editors in the Launchpad.

Target System Synchronization Module

- New columns `DPRShell.SupportedFeatureSet` and `DPRShell.Tags` for internal use.

Azure Active Directory Module

- Column `AADGroup.Description` extended to `nvarchar(1024)`.

Identity Management Base Module

- Column `AccProductGroup.Ident_AccProductGroup` 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 8.1.2 to version 8.1.3. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 56.

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 26.

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	changed
Cloud Systems Management Module	Universal Cloud Interface synchronization	none
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	changed
	Oracle E-Business Suite CRM data	none
	Oracle E-Business Suite HR data	none
	Oracle E-Business Suite OIM data	none
Microsoft Exchange Module	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2013/2016 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (v2)	changed
	Microsoft Exchange 2013/2016/2019 synchronization (v2)	changed
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	none
SAP R/3 User Management Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	none

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

Patches for synchronization projects

The following is a list of all patches provided for synchronization projects in One Identity Manager 8.1.3. 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 56.

Table 16: General patches

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

Table 17: Patches for Active Directory

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

Table 18: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#32844	Support for domain functional level Windows Server 2016	Adds the functional level to Windows Server 2016 domains.	32844
VPR#32871	Removes the negation of `TSInheritInitialProgram`	Corrects the mapping of the `edsaWTSUserConfigInheritInitialProgram` schema property in the `User` mapping because the value does not have to be negated anymore.	32871

Table 19: Patches for Oracle E-Business Suite

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

Table 20: Patches for Microsoft Exchange

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

Table 21: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#32781_NDO	Corrects the `DefaultUserPassword` variable	Corrects the security settings of the `DefaultUserPassword` variable.	32781

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

Table 22: Patches for Exchange Online

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

Table 23: Patches for SAP R/3

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

Table 24: Patches for SAP R/3 personnel planning data and structural profiles

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

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

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

Patches in One Identity Manager version 8.1.2

Table 26: 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 27: 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 28: 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	Corrects support of Oracle Database editions	Removes the `CP_EBSEdition` variable from the default variable set. This patch is applied automatically when One Identity Manager is updated.	30464

Table 29: Patches for Privileged Account Management

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

Patch ID	Patch	Description	Issue ID
		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 30: 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 31: 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 32: 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 33: 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 34: 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 35: 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 36: 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 37: 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 38: 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 39: 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 40: 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 41: 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 42: 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 43: Patches for Azure Active Directory

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

Table 44: 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 45: 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 46: 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 47: 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 48: 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 49: Patches for G Suite

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

Table 50: Patches for LDAP

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

Table 51: 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 52: 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 53: 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 54: 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 55: 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 56: Patches for SharePoint

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

Table 57: 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 58: 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 59: 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 60: Patches for Unix

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

Table 61: Patches for the One Identity Manager connector

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

Table 62: 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 NOTE: The cumulative update 2 for SQL Server 2019 is not supported. • Compatibility level for databases: SQL Server 2016 (130) • Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) NOTE: The SQL Server Enterprise Edition is strongly recommended on performance grounds.

Minimum requirements for the service server

Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating system Following versions are supported: • 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 63: 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

Connector	Supported data systems
	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 • 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, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, and 7.69 • SAP ECC 5.0 and 6.0 • SAP S/4HANA On-Premise-Edition
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the Authentication Services specifications.
IBM Notes connector	• IBM Domino Server versions 8, 9, and 10 • HCL Domino Server version 11 • IBM Notes Client 8.5.3 and 10.0 • HCL Notes Client Version 11.0.1
Native database connector	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA
Mainframe connector	• RACF • IBM i

Connector	Supported data systems
	• 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
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 Version 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 and 6.0

Product licensing

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

Upgrade and installation instructions

To install One Identity Manager 8.1.3 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 51.

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 8.1.3. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
  - Automatic software updating of version 7.0 to version 8.1.3 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 8.1.3 only works smoothly if the service pack 7.1.3 is installed.
- One Identity Manager uses In-Memory OLTP ((Online Transactional Processing) for memory optimized data access. The database server must support Extreme Transaction Processing (XTP). If XTP is not enabled, the installation or update will not start. Check whether the SQL Server property **Supports Extreme Transaction Processing** (IsXTPSupported) is set to **True**.

  The following prerequisites must be fulfilled to create memory-optimized tables:
  - A database file with the file type **Filestream data** must exist.
  - A memory-optimized data filegroup must exist.

  The Configuration Wizard checks whether these prerequisites are fulfilled before the One Identity Manager database can be installed or updated. The Configuration Wizard offers repair methods for creating the database file and database group.
- During the update of a One Identity Manager database version 7.0, 7.1 or 8.0 to version 8.1.3, 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 8.1.3 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 8.1.3, 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 8.1.3

IMPORTANT: Note the Advice for updating One Identity Manager on page 51.

To update an existing One Identity Manager installation to version 8.1.3

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 8.1.3, 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 8.1.3, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

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

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

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

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

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

   c. Click **Install**.

      This starts the installation wizard.

   d. Follow the installation instructions.

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

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

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

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

      sc description "HDBService" "One Identity Manager History Service"
      ```

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

10. Update other installations on workstations and servers.

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

To update synchronization projects to version 8.1.3

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 56.

To update an application server to version 8.1.3

- 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 8.1.3

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 8.1.3

- 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 8.1.3

- (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 8.1.3

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 24
- Patches for synchronization projects on page 26

Verifying successful installation

To determine if this version is installed

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

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

  The version number 2019.0001.0021.0300 for all modules and the application version 8.1 2019-01-21-317 indicate that this version is installed.

Additional resources

Additional information is available from the following:

- One Identity Manager Support
- One Identity Manager Online documentation
- One Identity Manager Community
- One Identity Manager Training portal website

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

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.