One Identity Manager 8.1.5

Release Notes

28 February 2022, 15:24

These release notes provide information about the One Identity Manager release, version 8.1.5. You will find all the modifications since One Identity Manager version 8.1.4 listed here.

One Identity Manager 8.1.5 is a patch release with new functionality and improved behavior. See New features on page 2 and Enhancements on page 3.

If you are updating a One Identity Manager version prior to One Identity Manager 8.1.4, 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

For the most recent documents and product information, see the One Identity Manager documentation.

About One Identity Manager 8.1.5

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 8.1.5:

Basic functionality

- The system information overview shows whether a database is encrypted.
- In the Database Compiler and in the program's status bar, a warning is shown if there are invalid script assemblies. The database needs to be compiled.
- To access the REST API on the application server, the user required the **Enables access to the REST API on the application server** (`AppServer_API`).

  > IMPORTANT: Ensure that the users that the ReST API communicates with, obtain this program function.

- The search index on the application server supports indexing of diacritical characters.
- To prevent maintenance tasks from obstructing daytime relevant post-processing in the DBQueue, a new `QBM_PDBQueueProcess_Mnt on <database>` database schedule has been implemented for processing the maintenance tasks. The maintenance tasks

pass your tasks on to the database schedule instead of running them themselves. This means that nothing changes in the scheduling of maintenance tasks. The database schedule does not have an active schedule, but is started through the `QBM_PWatchDog on <database>` database schedule.

- The effectiveness of the assignments (`XIsInEffect` column) is recorded in the history. Analysis of the effectiveness of the assignments in reports depends on the new **Common | ProcessState | PropertyLog | ShowEffectiveAssignmentsOnly** configuration parameter. If the configuration parameter is set, only the assignments in effect are shown in reports (default). If the configuration parameter is not set, all assignment are shown irrespective of their effectiveness.

  > NOTE: Assignment data that was recorded in an earlier One Identity Manager version is still shown irrespective of its current effectiveness.

Target system connection

- Support for One Identity Active Roles version 7.4.4.
- The Exchange Online connector uses the Exchange Online PowerShell V2 module.

See also:

- Enhancements on page 3
- Resolved issues on page 6
- Schema changes on page 32
- Patches for synchronization projects on page 34

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.1.5.

Table 1: General

Enhancement	Issue ID
Improved protection against damaging SQL statements.	33586, 33587
The Launchpad **Configure > Add system users** entry has been renamed to **Configure > Manage system users**.	33896
Columns of assignment tables (M:N tables, M:all tables) cannot be included in the full-text search (`DialogColumn.IndexWeight`). NOTE: To clean up existing installations, there is the **Column in m:n or m:all - table with IndexWeight > 0** consistency check that finds columns from assignment tables, which are weighted for the full-text	33976

Enhancement	Issue ID
index.	
In the Schema Extension, validity of the foreign key definition is checked when a read-only database view is added.	33320
Optimized performance importing schema extensions with the Database Transporter.	33797
In the Object Browser, when you switch to another object of the same type, the focus remains on the selected property. This makes it easier to compare object properties when you switch between them.	33843
Improved performance of various SQL functions.	33396
New mandatory field definitions for the `DialogState.Ident_DialogState`, `DialogState.NationalStateName`, `DialogCountry`.CountryName, `DialogCountry.NationalCountryName` columns. The groups of columns that must be unique (`QBMUniqueGroup`) have been adjusted.	34173
New optional parameter `-dc` (`--deleteconfig`) in the `InstallManager.CLI.exe` command line tool to remove configuration data and log files when uninstalling One Identity Manager.	33673

Table 2: General web applications

Enhancement	Issue ID
Logging in to the Web Portal with an OAuth provider is now possible without calling up oauth/{appId}/{authentifier} URL beforehand.	33553
Identity credentials (`id_token_hint`) are now passed during OAuth provider login.	33495
Improved Web Portal performance.	33328
It is now possible for a web application to communicate with an API Server other than the one that the web application comes from.	33841
The `withPermissions` parameter of the Web Designer `dbcount()` function is now marked as depreciated.	34222
Improved speed of displaying the shopping cart.	33913
Increased the Web Portal's security.	33611
Updated the `Microsoft.Owin` library to version 4.1.1.	33809

Table 3: Target system connection

Enhancement	Issue ID
This functionality, of access permissions automatically being created for clients when SAP roles or profiles are assigned to user accounts, was	33624

Enhancement	Issue ID
removed when ID 28147 was implemented in version 8.1.0. Now you are able to configure whether missing access to an SAP client is automatically allowed (entry in the `SAPUserInSAPMandant` table). To do this, the **TargetSystem | SAPR3 | AutoFillSAPUserMandant** configuration parameter has been introduced. If the configuration parameter is set, missing user account-client assignments are created after a role or a profile is passed down from this client. For direct assignments of roles and profiles, access to the client must be guaranteed beforehand as it was previously. ⚠ **CAUTION: By automating the inheritance process, user accounts might obtain access permissions for clients without the knowledge of the target system managers.** By default, the configuration parameter is not set.	
The `SAPUser.Guiflag` column's display name has been changed to **Login by SAP GUI allowed (insecure communication)**.	34251
SCIM filter expressions are passed down with each subset query during cursor-based paging.	33601
The SCIM connector now supports Bearer authentication for logging in to the target system. A patch with the patch ID VPR#33729 is available for synchronization projects	33729
Attribute check with schema during modification calls has been removed from the RACF connector.	33596
The native database connector now supports columns with the `DateTimeOffset` data type.	34214
The synchronization engine now differentiates between NULL and empty values when comparing.	33981
The Starling Cloud configuration wizard now supports the EU region in the One Identity Starling Cloud login. Users are automatically connected to the Starling Cloud system that suits them the best.	33748

Table 4: Identity and Access Governance

Enhancement	Issue ID
Improved performance calculating dynamic roles.	33675
Improved performance checking compliance rules.	33675
Improved performance in the queries that determine the approvers of default application procedures.	33997

See also:

- Schema changes on page 32
- Patches for synchronization projects on page 34

Resolved issues

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

Table 5: General

Resolved issue	Issue ID
Checking certificates of process steps with the `SendMail` and the `SendRichMail` process tasks fails if the revocation list distribution points defined in the certificate cannot be reached. The behavior has been changed as follows: If the revocation server is unreachable, the error will not occur. If the revocation server can be reached and the certificate is invalid, an error occurs.	33519

If the One Identity Manager database and the History Database are on different servers, an error may occur in certain circumstances.
`OLE DB provider... for linked server ... returned message "The object is in a zombie state. An object may enter a zombie state when either ITransaction::Commit or ITransaction::Abort is called, or when a storage object was created and not yet released.".`
`(0 rows affected) Msg 1206, Level 18, State 118, Procedure HDB_PGetRawFromSource_Intern, Line 581 [Batch Start Line 0] The Microsoft Distributed Transaction Coordinator (MS DTC) has cancelled the distributed transaction.`
	33541

In certain circumstances, when the Database Transporter is importing a transport package, the SQL session appears to get blocked. The messages are not updated soon enough in the Database Transporter. Therefore it looks like the transport package has not been processed.	33427
During bulk import of transport packages with the `DBTransporterCMD.exe` command line program, disabled triggers get left behind in the system.	33646, 33747, 34356
In the Schema Extension, not all 23 characters can be used for a table name (according to the documentation).	33552
In the Schema Extension, if a foreign key is created in the `BaseTree` table that points to a view (for example, `Locality`), the relation in the `QBMRelation` table is created incorrectly. As a result, the **QBMRelation invalid Child Execute by (RI)** consistency check fails.	33689

Resolved issue	Issue ID
The following error sometimes occurs when running various processes: `[810143] Database error 10054: A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`	33680
If a custom foreign key column is removed by the `QBM_PColumnCustomRemove` procedure, the generated RI triggers stay the same. These triggers still contain references to the columns that no longer exist.	33691
Missing permissions for custom schema extensions at database level after transporting more custom schema extensions. This issue occurs if the permissions have been granted manually.	33716
DBQueue Processor `QBM-K-CommonReIndexTable` tasks that reindex large tables do not disappear from the DBQueue. Reindexing of tables does not take place anymore if they are larger than 1 GB or have more than 1 million data records. Maintenance of these tables must be carried out by the database administrator within the maintenance period.	33733
DBQueue processing seems to halt, no more tasks are processed. In SQL Server reports, messages about blocking issues that the `QBM_PDBQueueProcess_Main` process session is involved in, are logged.	34132
The data in the `DialogTimezone`, `DialogCountry`, and `DialogState` tables is not up-to-date.	32980, 33181
The display values in templates are not resolved if the templates are calculated by a process step using the `ExecuteTemplates` process function. Running the template in an interactive session works correctly.	33769
Error calculating the initial, next activation time of the schedules. If a start date is defined for a new schedule, it is run for the first time not on this date but on the next scheduled date after this start date.	33836
SOAP Web Service methods that save do not work. If a method requires an object to be saved, this does not happen and the method does not have any effect, as in `PersonWantsOrg.MakeDecision`.	33915
If a CSV report is generated by a data stream that does not supply any data, the header is not written in the file. This creates an empty file. Solution: A new parameter, `CsvBandFilter`, for the `ReportComponent` process component's `Export` function, allows a header to be inserted even when the report does not have any data.	33971
Using the `SwitchToModuleGuid` function results in missing generic indexes.	34058

Resolved issue	Issue ID
If the **Only use for role-based authentication** option for a permissions group (`DialogGroup.IsRoleBasedOnly`) changes, the administrative users' members are not recalculated in this group. Solution: This option is always set for role-based permissions groups.	34098
When you edit change labels in the Designer and add several objects to one change label at the same time, the sort order is not correct. The object that you selected last, is inserted as the second object in the change label. For example, in the case of configuration parameters it might mean that during transport, the paths in the target database are not generated correctly.	33905
Error importing transport packages with extensions of database views and permissions respectively. If additional columns are created in a view definition's extension (`QBMViewAddOn`) and then permissions for them are granted and these changes are transported together, this error occurs during import: `[810143] Database error 50000: Cannot insert object in DialogColumnGroupRight because the associated object in DialogColumn does not exist. Rule QBM_RFRL27.`	33849
The `FileComponent` process component cannot set permissions on files and shares with a path length of more than 260 characters.	33512
If data query about the history of several objects uses an `XObjectKey` column from a parent query as criteria, it results in an empty set of results.	33539
Error reinitializing the One Identity Manager Service if there are orphaned process steps in the Job queue.	33558

Error when the One Identity Manager database was set up for replication. In this case, table are created by the SQL Server that do not conform to the One Identity Manager naming convention.
This causes the error:
`DBQueue task "QBM-K-SetRowLockOnly" fails with:`
`(execute slot single)50000 0 re-throw in Procedure QBM_ZSetRowLockOnly, Line 11`
`8152 0 detected in (SRV=..., DB=...) Procedure QBM_ZSetRowLockOnly, Line 3`
`8152 0 String or binary data would be truncated.`
Furthermore, some consistency checks also fail.
	33573

When modules are removed, references in dynamic foreign keys are not removed.	33638
Changing the password in the Launchpad causes errors when applications are started afterward.	33897

Resolved issue	Issue ID
Performance issues inserting a large number of objects if the table has a combination of columns that have to be unique. These issues particularly occur during initial synchronization.	34050
The control for editing process plan parameters in the Designer truncates the values.	34113
Loading Job queue processes is sometimes blocked by queries on tables that are locked by a transaction.	34136
In the Manager, the **Go to assigned object** context menu is enabled in drop-down menus in modal dialogs.	33340
In the Manager, the names of employees or organizations that begin with diacritical characters (such as Å, Ø or Æ) are not sorted in the **A-Z** or **Miscellaneous** filters.	33604
Very long process parameters are truncated and the process steps are not processed.	34236
When importing transport packages with system configuration, the necessary recalculation tasks are not created, which, for example, recreate the previously deleted FK constraints.	34252
When updating the database, the countries and capital Bhutan are not generated in national notation.	14013
In certain circumstances, no objects are imported from transport packages with change labels.	34331
Display error in the Database Transporter when exporting synchronization projects.	34379
Uninstalling One Identity Manager does not clear the entries in the registry.	33673

Table 6: General web applications

Resolved issue	Issue ID
The `TSBAERoleForGroup` view has bad performance. This leads to long delays when loading overview forms in the Web Portal.	32855
In the Web Portal, an error occurs if you open a date filter in a table, select a date and then cancel the whole process again.	33547
In the Web Designer, an object-dependent reference can no longer be edited after it has been saved, only deleted.	33982
In the Web Designer, an incorrect value is calculated in columns of `Int` data type in the `O3EMailbox` table when an action is performed.	34006
In Web Designer, the SQL query no longer uses a `select count (*)` to determine the total number of entries. This can lead to performance	34072

Resolved issue	Issue ID
problems. Solution: The `Count` function has been implemented again.	
In the Web Portal, a change to a support call under **Recently selected** by a staff member results in an error.	34131
In reports, the user who added an assignment is not always displayed.	34093
After adding a help archive in the Web Designer, the zip files are not found.	34199
If you open the list for selecting recipients at the beginning of a request process in the Web Portal, there is a loss in performance.	33693
When submitting a request in the Web Portal, an error message appears.	33705
In the `VI_Edit_Special_Person_TemporaryDeactivated` Web Designer component, the `IsTemporaryDeactivated` parameter cannot be set to **readonly**.	33800
In certain circumstances, long loading times occur in the Web Portal.	33845
When calling attestation functions in the Web Portal, there is a loss of performance.	34062
When creating a new report subscription in the Web Portal, it is not possible to close the dialog box with the **Escape** key.	33731, 33576
The swagger user interface is not accessible and the `Failed to load API definition.` error message appears.	33269
The API Server does not supply all JSON files in the HTML archives.	33282
In the Web Portal, the **Additional Columns** function is not displayed, although in Web Designer the corresponding columns of the collection have been marked as `IsAdditionalColumn=true`.	33625
When grouping delegations by the **Assignment Type** column in the Web Portal, the result list shows an incorrect number of delegations.	33791
The code generator creates an incorrect `TypedClient.ts` file that causes errors during compilation.	33881
In certain circumstances, date formats for attestations are not displayed in the user-defined format in Web Portal.	34094
Compilation of the **api-server-web-ui web** application quits unexpectedly.	34183
Certain special characters in the database password cause issues when installing the Web Portal.	34294
In certain circumstances, the Web Portal does not display the correct attestation policy of an attestation case in the pending attestation view.	33561

Resolved issue	Issue ID
Searching in the Web Portal in a large number of pending attestation cases (more than 1000) does not find all potential results.	33565
In certain circumstances, pending attestation cases are incorrectly displayed in the Web Portal.	33567
Attestation processes continue to be offered to persons for decision in the Web Portal, although their decision is no longer required.	33568
When editing or creating a report subscription in the Web Portal, if the list of selectable, additional subscribers also shows deactivated employees, an error occurs when saving the report subscription.	33580
If you create a new report subscription in the Web Portal, select additional subscribers and then create a new report subscription, the additional subscribers are preselected.	33635
In certain circumstances, in the Web Portal, the **View Settings** menu cannot be hidden using the Web Designer.	33659
When sending an inquiry about an attestation case to an user in the Web Portal, the respondent is incorrectly shown as authorized for approval.	33684
An employee incorrectly receives a message in the Web Portal when requesting a resource that they have already requested because the resource has already been directly assigned to the employee's subidentity.	33826
It is possible to edit business roles in the Web Portal that you do not manage.	33956
In certain circumstances, attestation cases are assigned to an incorrect attestation policy in the Web Portal.	34070
Too many identical SQL statements slow down the Web Portal.	34073
In the Web Portal, when filtering a large number of requests on the **Renew or Unsubscribe** page, not all potential requests are displayed.	34103
If the **VI_Common_SqlSearch_PrefixLike** configuration key is set, not all potential objects are found when searching in the Web Portal.	32680
In the Manager web application, the **Create assignment resource** task is provided for application roles and business roles	33526
Logging in to the Manager web application fails if TLS 1.2 is enabled and SSL 3.0 is disabled on the Internet Information Services. NOTE: By default, use of SSL is not set. SSL usage can now be optionally set. To do this, you must add the following entry in the Manager web application's configuration file (`Web.config`) in the section `application`. `<application>`	33670

Resolved issue	Issue ID

`    <add key="AllowSSL" value="True" />`
`</application>`	

When installing the Manager web application for the application pool, if a user is used whose password includes **&**, the Encrypt **web.config** step fails with the error: `An error occurred while parsing EntityName. Line 74, position 39.`	33831
Performance issues when viewing pending attestation cases in the Web Portal.	33662
If you want to use the **Check all services** function in the service availability check in the Operations Support Web Portal, an error occurs.	34204
If the values for additional request properties (`AccProductParameter`) are adjusted in the Web Portal by the approver during the approval process, these changes are not applied to the requests.	34092

Table 7: Target system connection

Resolved issue	Issue ID
An error occurs when connectors that use the local SQLite cache to load an object list and the virtual schema properties from the synchronization configuration with a property type of **Key resolution** are used. The value is a schema property is not correctly determined and the synchronization unexpectedly quits with am error. Error: `The object <obj> does not have a value for key property <prop>.`	33532
Performance issues in the target system browser when reloading objects from tables with more than one primary key and no object key.	33607
Incorrect logging of script variables in the synchronization log if a variable set other than the default one is used in the synchronization project.	33627
When a synchronization project is imported with the `DBTransporterCmd.exe` program, the shadow copy is not deleted. This means that after importing the synchronization project is opened in its old state.	33751
Error importing a synchronization project with the Database Transporter if the synchronization project already exists in the target database and several connected objects are deleted by the import.	33835
If an empty value cannot be resolved for a schema property of **Key resolution** type, a warning is logged or synchronization stops, depending on the configuration.	33877
Scripts for custom processing methods do not handle schema properties with values taken from the connected system. For example, if a custom processing method is run instead of the `Insert` method, the schema properties remain empty.	33979

Resolved issue	Issue ID
In custom processing method scripts, a third, optional parameter can now be given that passes the object value from the connected system.	
The value in the `XOrigin` column cannot be changed by synchronization.	33996
When publishing outstanding memberships in groups (`UNSAccountBInUNSGroupB`), the `HandleOutstanding` event is not triggered.	34023
Error during synchronization when properties needed for resolving object references are missing from the objects in the synchronization buffer.	34071
When native database columns are read or written with the native database connector, the date is converted to UTC.	33661
The native database connector does not take the reference scope into account if it is defined as a system filter only.	34257
Error connecting the SharePoint Online connector with the target system if legacy authentication with user name and password is disabled on the SharePoint server. Error: `[System.NotSupportedException] Cannot contact web site '<site>' or the web site does not support SharePoint Online credentials. The response status code is 'Unauthorized'.` TheSharePoint Online connector now supports authentication through an Azure Active Directory application with a self-signed certificate. A patch with the patch ID VPR#33432 is available for synchronization projects.	33432
Long runtimes for provisioning SharePoint Online user accounts, groups, roles, and permission levels.	33582
SharePoint Online connector performance issues. Error: "... has not been initialized."	33548
In the value list of the `O3SRole.RoleTypeKind` column, the values **Reviewer**, **RestrictedReader**, and **RestrictedGuest** are missing.	34074
In certain circumstances, Unix user accounts with special characters in their passwords are not added correctly. Only a fraction arrives in the target system. Provisioning ends with the error: `[Sugi.Common.Exceptions.SugiParserException] Received unexpected EOF while parsing action results`	33592
When a new Unix user account is created, the parameter for the home directory is not taken into account. This means that the home directory is always created under `/home/<user name>`.	33713
Error including a schema extension file in the SAP connector schema if the tables are defined after the functions in the file.	33564

Resolved issue	Issue ID
If a schema type is defined in a schema extension file that uses table definitions for the `ListObjectsDefinition` and `ReadObjectDefinition` attributes as well as function calls for the `InsertObjectDefinition`, `WriteObjectDefinition`, and `DeleteObjectDefinition` attributes, the parameters of the given function are missing in the resulting schema as schema properties of the schema type.	33574
Error when user accounts inherit SAP roles (`SAPUserInSAPRole`) if the corresponding SAP user account client access (`SAPUserMandant`) is marked as outstanding. Error 1: Although the **TargetSystem | SAPR3 | AutoFillSAPUserMandant** configuration parameter is not set or does not exist, valid assignments are generated. Error 2: If the **TargetSystem | SAPR3 | AutoFillSAPUserMandant** configuration parameter is set, valid assignments are generated. But the client's assignment to the user account stays outstanding. This provisions the role assignment. The outstanding mark is not removed until the next time synchronization is run. The `SAP_ZUserInSAPProfile` and `SAP_ZUserInSAPRole` procedures for calculating inheritance have been corrected. If the **TargetSystem | SAPR3 | AutoFillSAPUserMandant** configuration parameter is not set, the roles and profiles are not inherited by the user account and the entry in `SAPUserMandant` stays outstanding. If the **TargetSystem | SAPR3 | AutoFillSAPUserMandant** configuration parameter is set, the outstanding mark is removed and the roles and profiles are inherited by the user account NOTE: SAP roles and profiles can then also be assigned directly if the assignment to the user account of the client that the roles and profiles belong to, is marked as outstanding. This removes the outstanding mark.	33724
Passing parameter to functions that are defined in an SAP schema extension file is not always correct.	33939
Very long runtimes for calculating memberships in SAP roles in One Identity Manager version 8.1.4.	33959
The SAP synchronization project consistency check shows warning messages. A patch with the patch ID VPR#33980 is available for synchronization projects.	33980
When renaming SAP user accounts in the Manager, the **Disabled password** option is not taken into account.	34059
The `SAPUserInSAPHRP.Excluded` column is not provisioned in SAP R/3 although it can be edited in the Manager. A patch with the patch ID VPR#34081 is available for synchronization	34081

Resolved issue	Issue ID
projects.	
The description of SAP roles is divided into two fields in the SAP GUI. In One Identity Manager, the entire description is written in one column although there are also two fields available. In the synchronization project, a new virtual schema property has been created to divide up the description. The map has been adapted. A patch has been provided to correct existing synchronization projects.	34128
An SAP group can be assigned to SAP user accounts that are administered through a Central User Administration, in One Identity Manager only if the group's client is assigned to the user accounts. In the SAP R/3 environment, a user account can be assigned to the central client's group without the user account being authorized for the central client.	34164
Error provisioning an SAP user account when the valid from date of the user account is greater than the valid until date. This data installation is now prevented in One Identity Manager.	34245
Exchange Online dynamic distribution groups (`O3EDynDL` table) do not allow the empty included recipients (`IncludedRecipients` column) although it is not a mandatory field in the Exchange Admin Center. An error occurs during synchronization. The Customizer prevents the column from being empty.	33730
Incorrect number of the Notes version in log messages when using IBM Domino Server version 10 or HCL Domino Server version 11.	33654
Error provisioning Notes mail-in databases.	33755
When a mail-in database is created, it is mandatory to enter the Notes domain that the mail-in database should belong to. There is a property mapping rule missing for transferring the value to the target system during provisioning of the mail-in database. A patch with the patch ID VPR#33759 is available for synchronization projects.	33759
The IBM Notes connector does not store the user ID file in the location specified in the **TargetSystem | NDO | TempNetworkPath** configuration parameter. The configuration parameter has been deleted. Customized usage might require modification. Use the settings in the main data of the linked Notes domain or the allocated mail server.	34302
When the system connection to an Oracle E-Business Suite is saved, parts of the connection credentials are saved twice. A patch with the patch ID VPR#34008 is available for synchronization projects.	34008

Resolved issue	Issue ID
If an Active Directory global catalog is unreachable due to the firewall configuration, requests to the global catalog will not fail. Process steps that perform name resolution through a global catalog remain in the **Processing** state in this case. Solution: A timeout of **65** seconds has been built into the Active Directory connector so that a request that is not answered within a certain time is considered to have failed.	33807
When creating Active Directory user accounts, diacritical characters (for example, Å, Ø, or Æ) are not correctly taken into consideration in the templates and table scripts. The user accounts are not created.	33590
The description of the **TargetSystem | ADS | Accounts | NotRequirePassword** configuration parameter does not match the behavior. The description has been adjusted.	33500
Errors in the documentation of some Password Capture Agent properties in the *One Identity Manager Password Capture Agent Administration Guide*.	33967
Errors may occur when synchronizing LDAP groups and their members if at least one member user account is not yet stored in the One Identity Manager database and is only found in the synchronization buffer.	34211
Assigning an LDAP computer to a device does not queue a `LDP-K-LDPMachineInLDAPGroup` recalculation task. This means that groups inherited through the device are not assigned to the computer.	33509

Error when provisioning memberships in LDAP groups. An attempt is made to write a empty value to the `Member` attribute of an LDAP group.
Error message:
`Operation error message: A protocol error occurred.`
`Response result code: (2) ProtocolError`
`Response message: no values given`
	33869

Issues if the `Password` property is a mandatory field in LDAP. For all schema classes that have this property, a `vrtPassword` is provided by the connector. The virtual property is mapped in the default. The actual `Password` property is not mapped. This leads to an error in the consistency check of the synchronization project as well as errors in provisioning.	34091
The length of the `LDAPAccount.RoomNumber` column is too short.	34099

An error occurs when checking an Active Directory password policy in the Designer:
`VI.DB.DatabaseException: Database error 1: SQL logic error`
`no such table: ADSPolicyAppliesTo`
	33770

Resolved issue	Issue ID
The **Custom** and the **User defined** tabs on the main data form for cloud user accounts are both called **Custom** in the English user interface.	33578
Error synchronizing a cloud application with the SCIM connector when using the `ETAG` property as a revision counter.	33762
Not all changed objects are correctly viewed and updated when synchronizing a cloud application with revision filtering because the time zone of the SCIM provider is not taken into account.	33949
Exception error during initial synchronization of a cloud application with the SCIM connector: Invalid token header. No credentials provided.	33988
Authentication failure due to missing encoding when logging in to an Oracle cloud application using the SCIM connector.	34123
The length of the `AADUser.State` column is too short.	33954
Performance problems during synchronization if many-to-all tables are included in the mapping.	34096
Simultaneous provisioning of multiple G Suite organizations fails (quota exceeded).	33636
The Customizer prevents the primary email address of a G Suite user account from being changed if this involves using an email address that is already assigned as an alias.	34160
The Customizer prevents the modification of Microsoft Exchange mailboxes when the Active Directory user account is disabled.	34329
When exiting the System Connection Wizard for Microsoft Exchange, an error occurs if a password with two dollar signs ($) is entered in the connection parameters. Error message: `Unknown Variable (T)!`	34359
The `Delete sensitive data` process step does not always run reliably when the employee's central password is propagated to the user account. It might result in password fields in the database not being cleared. The behavior has been changed as follows: • An employee's central password is now only passed on to user accounts belonging to target systems that are synchronized by the One Identity Manager (`NamespaceManagedBy=VISYNC`). In custom target systems, it must also be possible to perform write operations (`IsNoWrite=0`). • For read-only target systems (`NamespaceManagedBy=ReadOnly`), the employee's central password is no longer propagated to the employee's user accounts.	32671

Resolved issue	Issue ID

• An additional process step has been implemented in the processes for user accounts. This waits until all user account's processes have completed. Then the user account's password data is deleted from the database.
The following processes were modified:
`AAD_User_Insert`
`AAD_User_Update/(De)Activate`
`ADS_ADSAccount_Insert`
`ADS_ADSAccount_Update/(De-)activate`
`ADS_ADSAccount_Insert (ReadOnly)`
`LDP_Account_Insert`
`LDP_Account_Update/(De-)Activate`
`CSM_User_Insert`
`CSM_User_Provision`
`EBS_EBSUser_Insert`
`EBS_EBSUser_Update`
`GAP_User_Insert`
`GAP_User_Update/(De)Activate`
`PAG_User_Insert`
`PAG_User_Update/(De)Activate`
`SAP_SAPUser_Insert`
`SAP_SAPUser_Update`
`UNX_Account_Insert`
`UNX_Account_Update/(De)activate`
`NDO_NDOUser_Insert`
`NDO_NDOUser_Update`
`NDO_NDOUser_Insert (ReadOnly)`
`UCI_UCIUser_Insert`
`UCI_UCIUser_Update`	

Changing an employee's central password several times quickly results in an error. Error: `<Central Account> was changed by another user.`	34388

Table 8: Identity and Access Governance

Resolved issue	Issue ID
When calculating whether the an approval step has timed out for an approver or attestor, the members of the chief approval team are taken into consideration. This may result in the approval step not being escalated or broken off although the timeout has been exceeded for all the regular approvers.	33436
If attestation cases for permanently deactivated employees are closed automatically, no publishing date (`DateHead`) is set.	33511
If there are several thousand **Reminder for attestation cases** tasks being processed in the DBQueue, blocked sessions and deadlocks may occur. This prevents the DBQueue from being processed quickly.	33570
If several attestors have been determined for one approval step where the number of approvers is set to 1 and one attestor has already made an approval decision, the other attestors are still sent a reminder email. This error occurs in the scheduled demand for attestation.	33664
Attestation cases do not come to an end when attestations for several attestation policies are started simultaneously and generation of an attestation case fails.	33711
Performance issues approving attestation cases.	33732
Very high memory usage and performance issues running attestations for attestation policies that create a lot of attestation cases. Solution: 1. Transaction repetition has been disabled in the objects layer. Now there might be more error messages during processing. 2. The `VI_GetAttestationObject` script can be customized. An optimized version that only contains the foreign key references can significantly reduce the runtime.	33994
If the approval policy that applies to a product is defined on the service item or the service category, the product cannot be moved without breaking off any active requests.	33650
Error unsubscribing a product with a limited period. If the request of a limited period product has been renewed several time such that the total validity period exceed the validity period define in the service item, an error occurs when unsubscribing the product.	33756
Double entries in the `PWOHelperPWO` table. Sporadically, entries in the auxiliary table for request procedures (`PWOHelperPWO`) are add twice. This leads to a doubling of email notifications. If the approval workflow contains an approval step for external approval, the process for external approval is generated twice.	33780

Resolved issue	Issue ID
Renewing a limited period request fails although the renewal's expiry date is withing the validity period.	33892
The main data forms for departments, locations, cost centers, and business roles also show countries that are not enabled in the **Country** menu. Only enabled countries are allowed.	33668
Assignments created through inheritance of SAP roles and SAP user accounts become active one day late. This happens if the database server is in a timezone to the west of UTC.	34034
In One Identity Manager, if the validity period of an SAP user account is changed, no recalculation of company resource assignments to employees is triggered.	34338
New keywords for service items will only be found after a complete re-indexing has been performed on the application server.	33518
For automatic approvals, the processes do not go to the **Frozen** status when they fail.	33386
Error saving completed requests if a validity period (**Max. days valid**) is subsequently set on the service item.	33799
When approving requests, an error occurs under the following conditions: • The approval has been delegated and the delegator would like to be notified of the approval decision. • The reason for the approval decision is too long.	33861
A request for recalculating the approvers is queued in the DBQueue, although the **NoRecalc** is set on the **QER | ITShop | ReducedApproverCalculation** configuration parameter.	33932
Renewals and cancellations fail if the request's valid until date has already passed at the time of approval.	33935
It is not possible to reduce the value of **Max. days valid** for a single service position. Changes to this value now affect new requests and renewals. If the value is changed from **0** to greater than **0**, the change also affects existing requests.	34038
Requests receive the status **Pending** after final approval, although no other request is active.	34052
If a cancellation date that is in the past is specified for a cancellation, an error message appears. Subsequently, the product cannot be canceled even with a valid date.	34144
On the overview forms of resources and service items, columns that do not exist are used in the **Display columns** property	33674

Resolved issue	Issue ID
(`DialogTree.ElementColumns`).	
If an exclusion clause is defined for two business roles (`BaseTreeExcludesBaseTree`), it may happen that a dynamic role should nevertheless assign a employee to the business role. The DBQueue Processor assignment is not processed and an error is logged: `Cannot make assignment because there are already employee assignments to roles that exclude the roles to be added.`	33720
If a new employee is created in the Manager or the Web Portal and the manager (`UID_PersonHead`) is entered at the same time, the process defined in the `HelperHeadPerson` table that is supposed to start by setting the manager, is not triggered.	34063
Missing indexing for the `BaseTreeOwnsObject` table.	34130
Incorrect German translation for the entry `The following employees are currently entitled to approve this request.`	34175
When approving rule violations, exception approvers can specify a valid until date that exceeds the validity period specified in the compliance rule.	33808
The employee group affected by a compliance rule is determined incorrectly, if main and subidentities need to be determined.	34197
When deserializing objects of an attestation case, an error may occur if the logged in user does not have sufficient edit permissions.	34365

Table 9: IT Service Management

Resolved issue	Issue ID
In the Manager, it is not possible to maintain the number of CPUs per computer or server	33745

See also:

- Schema changes on page 32
- Patches for synchronization projects on page 34

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

Known Issue	Issue ID
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.	
The default settings of `globallog.config` assume that write permissions exists for `%localappdata%`. If an EXE does not have sufficient permissions, the log can be written to a directory that does have the access permissions 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. If a `Save Transaction` is run in the process, an error occurs: `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: • The cumulative update 2 for SQL Server 2019 is not supported. For more information, see https://support.oneidentity.com/KB/315001.	32814

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

Known Issue	Issue ID
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

If the application is supplemented with custom DLL files, an incorrect version of the `Newtonsoft.Json.dll` file might be loaded. This can cause the following error when running the application:
`System.InvalidOperationException: Method may only be called on a Type for which Type.IsGenericParameter is true.`
`at System.RuntimeType.get_DeclaringMethod()`
There are two possible solutions to the problem:
• The custom DLLs are compiled against the same version of the `Newtonsoft.Json.dll` to resolve the version conflict.
• Define a rerouting of the assembly in the corresponding configuration file (for example, `web.config`).
Example:
`<assemblyBinding >`
`<dependentAssembly>`
`<assemblyIdentity name="Newtonsoft.Json"`
`publicKeyToken="30AD4FE6B2A6AEED" culture="neutral"/>`
`<bindingRedirect oldVersion="0.0.0.0-11.0.0.0"`
`newVersion="11.0.0.0"/>`
`</dependentAssembly>`
	33867

Known Issue	Issue ID
`</assemblyBinding>`	
In the Web Portal, the details pane of a pending attestation case does not show the expected fields if the default attestation procedure is not used, but a copy of it is. Solution: - The object-dependent references of the default attestation procedure must also be adopted for the custom attestation procedure.	34110

Table 12: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use `Import-PSSession` internally.	23795
By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely. Solution: Make it possible to access the building block **HR_ENTRY_DATE** remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate` in the Synchronization Editor.	25401
Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses were stored up to now.	27042
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
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.	27687

Known Issue	Issue ID
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.	
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. - OR - • A company is assigned to the central system.	29253
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.`	796028, 30963

Known Issue	Issue ID
The request is denied in One Identity Manager and the error in the request is displayed as the reason.	
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. - OR - • Disable the cache in the file `VI.Projector.SharePoint.<Version>.Host.exe.config`.	31017
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:
	32149

Known Issue	Issue ID

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

There are no error messages in the file that is generated in the `PowershellComponentNet4` process component, in `OutputFile` parameter. Cause: No messages are collected in the file (parameter `OutputFile`). The file serves as an export file for objects returned in the pipeline. Solution: Messages in the script can be outputted using the *> operator to a file specified in the script. Example: `Write-Warning "I am a message" *> "messages.txt"` Furthermore, messages that are generated using `Write-Warning` are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an `Exception`. This message then appears in the One Identity Manager Service's log file.	32945
The G Suite connector cannot successfully transfer Google applications user data to another G Suite user account before the initial user account is deleted. The transfer fails because of the Rocket application's user data. Workaround: In the system connection's advance settings for G Suite, save an application transfer XML. In this XML document, limit the list to the user data to be transferred. Only run the Google applications that have user data you still need. You can see an example XML when you edit the application transfer XML in the system connection wizard. ***To limit the list of user data you want to transfer*** 1. In the Synchronization Editor, open the synchronization project. 2. Select **Configuration** > **Target system**. 3. This starts the system connection wizard. 4. On the system connection wizard's start page, enable **Show advanced options**. 5. On the **Advanced settings** page, enter the XML document in the **Application transfer XML** field. 6. Save the changes.	33104
If target system data contains appended spaces, they go missing during synchronization in One Identity Manager. Every subsequent synchronization identifies the data changes and repeatedly writes the affected values or adds	33448

Known Issue	Issue ID
new objects if this property is part of the object matching rule. Solution: Avoid appending spaces in the target system.	
If the user's password that the native database connector uses to log in on the SAP HANA database expires soon, the SAP HANA system sends a warning. This results in the connector not being able to log in on the target system even before the password has expired. The connection attempt is canceled and an error message is displayed. Error message: `Sap.Data.Hana.HanaException: user's password will expire within few days` Solution: Ensure the following for the user that the native database connector uses to log in on the SAP HANA database. • A valid password is always stored for the user in the SAP HANA database and in the synchronization project. • The warning period for expiring passwords is never reached by this user.	34419

Table 13: Identity and Access Governance

Known Issue	Issue ID
Moving a shelf to another shop and the recalculation tasks associated with it can block the DBQueue. Solution: Parent IT Shop nodes of shelves and shops cannot be changed once they have been saved. ***To move a product in a shelf to another shop*** • Select the task **Move to another shelf**. - OR - • Assign the product to a shelf in the new shop then remove the product assignment to the previous shelf. Once you have moved all the products, you can delete the shelf.	31413
During approval of a request with self-service, the `Granted` event of the approval step is not triggered. In custom processes, you can use the `OrderGranted` event instead.	31997

Table 14: Third party contributions

Known Issue	Issue ID
An error can occur during synchronization of SharePoint websites under SharePoint 2010. The method `SPWeb.FirstUniqueRoleDefinitionWeb()` triggers an `ArgumentException`. For more information, see https://support.microsoft.com/en-us/kb/2863929.	24626
Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting **File and Printer sharing** is not set on the server. This option is not set on domain controllers on the grounds of security.	24784
An error, TNS-12516, TNS-12519 or ORA-12520, sporadically occurs when connecting with an Oracle Database. Reconnecting normally solves this. Possible cause: The number of processes started has reached the limit configured on the server.	27830
Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages. Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.	29051
Valid CSS code causes an error under Mono if duplicate keys are used. For more information, see https://github.com/mono/mono/issues/7455.	762534, 762548, 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.`	31995

Known Issue	Issue ID
`at System.Security.Cryptography.NCryptNative.CreatePersistedKey (SafeNCryptProviderHandle provider, String algorithm, String name, CngKeyCreationOptions options)` For more information, see https://support.microsoft.com/en-us/help/4014602. Workaround: 1. In the Internet Information Services (IIS) Manager, select the application and then the **Advanced Settings** context menu item. 2. On the **Process Model** panel, set the option **Load User Profile** to **True**.	
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 Microsoft code with the Visual Basic .NET 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 8.1.4 up to version 8.1.5.

Azure Active Directory Module

- `AADUser.State` column extended to `nvarchar(128)`.

Exchange Online Module

- New mandatory field definition for the `O3EDynDL.IncludedRecipients` column.

LDAP Module

- `LDAPAccount.RoomNumber` column extended to `nvarchar(64)`.

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 8.1.4 to version 8.1.5. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 68.

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 34.

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	none
Active Roles Module	Synchronize Active Directory domain via Active Roles	changed

Module	Synchronization template	Type of modification
Cloud Systems Management Module	Universal Cloud Interface synchronization	none
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	none
	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)	none
	Microsoft Exchange 2013/2016/2019 synchronization (v2)	none
G Suite Module	G Suite synchronization	none
LDAP Module	AD LDS synchronization	none
	OpenDJ synchronization	none
IBM Notes Module	Lotus Domino synchronization	changed
Exchange Online Module	Exchange Online synchronization (deprecated)	none
	Exchange Online synchronization (v2)	none
Privileged Account Governance Module	One Identity Safeguard synchronization	none
SAP R/3 User Management Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	none
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	none
SAP R/3 Compliance Add-on Module	SAP R/3 authorization objects	none
SAP R/3 Structural Profiles Add-on Module	SAP R/3 HCM authentication objects	changed

Module	Synchronization template	Type of modification
	SAP R/3 HCM employee objects	none
SharePoint Module	SharePoint synchronization	none
SharePoint Online Module	SharePoint Online synchronization	changed
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 8.1.5. 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 68.

Table 16: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#33729	Support for Bearer authentication	Adds a variable for using the Bearer token as a connection parameter. This patch is applied automatically when One Identity Manager is updated.	33729

Table 17: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#34008	Clearing up connection parameters	Removes unnecessary system connection parameters from the connection parameter. This patch is applied automatically when One Identity Manager is updated.	34008

Table 18: Patches for IBM Notes

Patch ID	Patch	Description	Issue ID
VPR#33759	Corrected **Database** map	Adds a property mapping rule for the `MailDomain` schema property in the **Database** map. This patch is applied automatically when One Identity Manager is updated.	33759

Table 19: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#33432	Support for authenticating through an Azure Active Directory application	Add variables for supporting authentication through an Azure Active Directory application to the connection parameter.	33432

Table 20: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#33980	Changes to the reference scope for the `SAPSystem` schema type	Extends the reference scope with a condition for SAP systems and corrects some property mapping rules. This patch is applied automatically when One Identity Manager is updated.	33980
VPR#34128	Corrected the **role** map for describing SAP roles	Divides the description of SAP roles between the `Description` and the `RoleDescription` schema properties.	34128

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

Patch ID	Patch	Description	Issue ID
VPR#34081	Corrects the **userInSProfile** map for the `Excluded` schema property	Changes the mapping of the `Excluded` schema property so that changes are written to the target system.	34081

Patches in One Identity Manager version 8.1.4

Table 22: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#33399	Filters the	Adds a member filter for user accounts in	33399

Patch ID	Patch	Description	Issue ID
	members of administrator roles	the **vrtMember_Members** property mapping rule in the **DirectoryRole** map. This patch is applied automatically when One Identity Manager is updated.	

Table 23: Patches for Oracle E-Business Suite

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

Table 24: Patches for Exchange Online

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

Table 25: Patches for SAP R/3

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

Table 26: Patches for the SCIM interface (in Universal Cloud Interface Module)

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

Patches in One Identity Manager Version 8.1.3

Table 27: 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 28: 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 29: 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 `edsaWTSUserConfigInheritInitialProgram` in the `User` map because the value does not need to be negated anymore.	32871

Table 30: 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 31: 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 32: Patches for IBM Notes

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

Table 33: 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 34: Patches for SAP R/3

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

Table 35: 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 36: 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 37: 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 38: Patches for Exchange Online

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

Table 39: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#32667	Deletes the alternative objects mapping rules from the **oRA-**	Deletes the object mapping rule **Identifier <-> REQUEST_GROUP_ID** from the **oRA-**	32667

Patch ID	Patch	Description	Issue ID
	Requestgroup mapping	**Requestgroup** mapping. This patch is applied automatically when One Identity Manager is updated.	
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 40: 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. 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.	32031
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 41: 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 42: 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 43: 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 44: 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 45: 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 46: Patches for Exchange Online

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

Table 47: 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.	31794

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

Table 48: 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 49: 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.	31568

Patch ID	Patch	Description	Issue ID
		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.	
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 for session access (part 1)	An access request policy can have multiple directory accounts for session access. Prerequisite for patch **AccessRequestPolicy model changes for session access (part 2)**. This patch is applied automatically when One Identity Manager is updated.	31664
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	31703

Patch ID	Patch	Description	Issue ID
		when One Identity Manager is updated.	
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 50: 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.	31796

Patch ID	Patch	Description	Issue ID
		This patch is applied automatically when One Identity Manager is updated.	
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 51: 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 52: 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 53: 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 54: Patches for Azure Active Directory

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

Table 55: 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 56: 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 57: 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 58: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#28815	Extends a processing method in the synchron-	Extends the processing method `MarkAsOutstanding` in the	28815

Patch ID	Patch	Description	Issue ID
	ization step RoleAssignmentPolicy	synchronization step RoleAssignmentPolicy.	
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 59: 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 60: Patches for G Suite

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

Table 61: Patches for LDAP

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

Table 62: 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 63: Patches for SAP R/3

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

Patch ID	Patch	Description	Issue ID
		updated.	
	Milestone 8.1	Milestone for the context **SAP R/3**.	

Table 64: 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 65: 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 66: 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 67: Patches for SharePoint

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

Table 68: 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 automat-	30729

Patch ID	Patch	Description	Issue ID
		ically when One Identity Manager is updated.	
	Milestone 8.1	Milestone for the context **SharePoint Online**.	

Table 69: 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 70: 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 71: Patches for Unix

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

Table 72: Patches for the One Identity Manager connector

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

Table 73: 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 **TargetSystem | NDO | TempNetworkPath** configuration parameter has been deleted.

  Customized usage might require modification. Use the settings in the main data of the linked Notes domain or the allocated mail server.

- 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 with 2.5 GHz+ frequency (non-production) 16 physical cores with 2.5 GHz+ frequency (production) NOTE: 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM (non-production) 64 GB+ RAM (production)
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. NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems. - Compatibility level for databases: SQL Server 2016 (130) - Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended)

> NOTE: The minimum requirements listed above are considered to be for general use. With each custom One Identity Manager deployment these values may need to be increased to provide ideal performance. To determine production hardware requirements, it is strongly recommended to consult a qualified One Identity Partner or the One Identity Professional Services team. Failure to do so may result in poor database performance.
>
> For additional hardware recommendations, read the KB article https://support.oneidentity.com/identity-manager/kb/290330/how-to-configure-settings-as-per-the-system-information-overview, which outlines the System Information Overview available within One Identity Manager.

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 NOTE: In newer versions of Mono, starting with version 6.10, set the `MONO_PATH` environment variable explicitly to the current install directory to ensure that all referenced assemblies can be loaded.

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 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 74: 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 (Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names) and RFC 4512 (Lightweight Directory Access Protocol (LDAP): 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

Connector	Supported data systems
	configuration to write data to the Web Service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active Directory connector	Active Directory, shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.
Microsoft Exchange connector	• Microsoft Exchange 2010 Service Pack 3 or later • Microsoft Exchange 2013 with cumulative update 23 • 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, 7.54, 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 specifications for One Identity Safeguard Authentication Services.
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

Connector	Supported data systems
Mainframe connector	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 6.9, 7.0, 7.2, 7.3.1, 7.3.3, 7.4.1, 7.4.3, and 7.4.4
Azure Active Directory connector	• Microsoft Azure Active Directory NOTE: Synchronization of Azure Active Directory tenants in national cloud deployments with the Azure Active Directory connector is not supported. This affects: • Microsoft Cloud for US Government • Microsoft Cloud Germany • Azure Active Directory and Microsoft 365 operated by 21Vianet in China 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. They must conform to RCF 7643 (System for Cross-domain Identity Management: Core Schema) and RFC 7644 (System for Cross-domain Identity Management: Protocol).
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	• One Identity Safeguard Version 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11

Connector	Supported data systems
Safeguard connector	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 8.1.5 for the first time, follow the installation instructions in the *One Identity Manager Installation Guide*. For more detailed instructions about updating, see the *One Identity Manager Installation Guide*.

> IMPORTANT: Note the Advice for updating One Identity Manager on page 62.

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 8.1.5. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
    - Automatic software updating of version 7.0 to version 8.1.5 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 8.1.5 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 8.1.5, 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 8.1.5 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 8.1.5, 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 Database before updating your One Identity Manager History Service. Run the following command as administrator:

  ```
  sc delete "HDBService"
  ```

- Once this version has been installed, users that need to access the REST API in the application server require the **Enables access to the REST API on the application server** (`AppServer_API`) function. Assign this program function to the users. For more information, see the *One Identity Manager Authorization and Authentication Guide*.

Updating One Identity Manager to version 8.1.5

> IMPORTANT: Note the Advice for updating One Identity Manager on page 62.

To update an existing One Identity Manager installation to version 8.1.5

1. Run all the consistency checks in the Designer in **Database** section.
   1. Start the Consistency Editor in the Designer by selecting the **Database** > **Check data consistency** menu item.
   2. In the **Test options** dialog, click AZ↓.
   3. Under the **Database** node, enable all the tests and click **OK**.
   4. To start the check, select the **Consistency check** > **Run** menu item.

      All the database tests must be successful. Correct any errors. Some consistency checks offer repair options for correcting errors.
2. Update the administrative workstation, on which the One Identity Manager database schema update is started.
   1. Execute the program `autorun.exe` from the root directory on the One Identity Manager installation medium.
   2. 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**.
   3. 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 8.1.5, 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 8.1.5, 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 8.1.5

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

   > NOTE: Some patches are applied automatically. A process that migrates all existing synchronization project is queued in the Job queue to do this. To execute the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

   - Check whether the `DPR_Migrate_Shell` process has been started successfully.

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

For more information, see Applying patches to synchronization projects on page 68.

To update an application server to version 8.1.5

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

To update the Web Portal to version 8.1.5

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

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

To update an API Server to version 8.1.5

- 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 8.1.5

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

To update the Manager web application to version 8.1.5

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

Applying patches to synchronization projects

> ⚠ CAUTION: **Patches do not alter custom changes in synchronization projects. This means that conflicts may occur if patches are applied to synchronization projects that have been customized. It may cause loss of data.**
>
> ***Before you apply a patch***
>
> 1. **Read the patch description to decide whether it provides the necessary improvements for the synchronization project.**
> 2. **Check whether conflicts with customizations could occur.**
> 3. **Create a backup of the database so that you can restore the original state if necessary.**
> 4. **Deactivate the synchronization project.**

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

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

To apply patches

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Edit** > **Update synchronization project** menu item.
3. In **Available patches**, select the patches you want to apply. Multi-select is possible.

   In **Details - Installation summary**, all patches are displayed in order of installation.
4. Click **Apply selected patches**.
5. Enter any user input as prompted.
6. Use the patch log to check whether customization need to be reworked.
7. If required, rework customizations in the synchronization configuration.
8. Run a consistency check.
9. Simulate the synchronization.
10. Activate the synchronization project.
11. Save the changes.

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

the changes.

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

See also:

- Modified synchronization templates on page 32
- Patches for synchronization projects on page 34

Verifying successful installation

To determine if this version is installed

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

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

  The version number 2019.0001.0021.0500 for all modules and the application version 8.1 2019-01-21-563 verify that this version is installed.

Additional resources

Additional information is available from the following:

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

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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