One Identity Manager 9.1

Release Notes

15 September 2022, 09:38

These release notes provide information about the One Identity Manager release, version 9.1. You will find all the modifications since One Identity Manager version 8.2.1 listed here.

One Identity Manager 9.1 is a minor release with new functionality and improved behavior. See New features on page 2 and Enhancements on page 8.

If you are updating a One Identity Manager version older than One Identity Manager 8.2.1, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under One Identity Manager Support.

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

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

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

About One Identity Manager 9.1

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 company 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.

One Identity Starling

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 One Identity Starling. For a free trial of our One Identity Starling offerings and to get the latest product feature updates, visit https://www.cloud.oneidentity.com.

New features

New features in One Identity Manager 9.1:

General

- Azure SQL Database is supported.

  NOTE: An Azure SQL Database must be available to install the schema. There is no support for creating a new Azure SQL Database with the Configuration Wizard.
- Internal DBQueue Processor tasks are processed by a service, the Database Agent Service. The Database Agent Service is deployed by a One Identity Manager Service plugin. The DatabaseAgentPlugin must be configured on the Job server that serves as the update server. An administrative user must be used for the database connection in the Job provider. Alternatively, the Database Agent Service can be run by the `DatabaseAgent.exe` command line program.
- The Configuration Wizard provides support for deleting a One Identity Manager database. Deleting a database also removes the database users, database roles, and server roles, as well as SQL Server logins.

- The Configuration Wizard provides you with support for enabling a restored database. The necessary database users, database roles, and server roles are created and the database is compiled.
- Due to security issues, you cannot run any database queries directly from the user interface or from web applications. Specific SQL operators undergo a risk assessment that prevents them from being used by One Identity Manager components. This includes operators such as `LIKE`, `NOT LIKE`, `<`, `<=`, `>`, or `>=`.

  In order to continue using certain features in One Identity Manager components, users require the **Common_AllowRiskyWhereClauses** program function.

  Users who do not have this program function can only run database queries that are classified as trusted or pose no risk. Some of the features in One Identity Manager components, such as testing dynamic roles or running filter queries, are not possible without this function. For more information, see the *One Identity Manager Authorization and Authentication Guide*.
- The **SessionHttpAuthentication** plugin for the One Identity Manager Service supports logging in on the service's website with authentication modules. The users still require the **JobServer_Status** program function.
- Support for disabling WHERE clauses for the application server REST API.
- Various password columns have been extended.
- You can enter an additional description for password requirements that are checked in the test script for password policies. This is displayed in the password policy description in the Password Reset Portal.
- System users can be blocked from logging in directly to One Identity Manager tools.
- A new **User account (manual input/role-based)** authentication module is provided. The employee whose login data matches that of the current user is used for logging in.
- Authentication modules for the Password Reset Portal can use a list of columns from the same table to search for a user.
- In the Database Transporter, several transport packages can now be combined into one cumulative transport package. If individual transport packages require the database to be compiled, the web projects are not complied until each of the transports from the cumulative transport package have been imported.
- To re-enable process steps with the **Frozen** status in Job Queue Info, users need the **JobQueue_Frozen** program function.
- Search index optimization can be started manually on the application server.
- A connection timeout can be set in the One Identity Manager tools default connection dialog.
- New optional parameter in the `DBCompilerCMD.exe` command line program to compile only those parts of the system that have changed.
- New process function `Execute SQL Single` for the `SQLComponent` process component to run SQL statements in a single instance. The process function can be used when a special procedure call or a special data change is explicitly allowed to run just in one

instance.

- A script for changing values can be stored with the parameters (`DialogParameter.OnPropertyChangedScript`), which dynamically determines whether a parameter is, for example, read-only or mandatory.
- Integration of events into typed wrapper classes.
- Support for NLog 5.0.
- Support for Microsoft .NET Framework version 4.8.
- The One Identity Manager History Database has been significantly simplified in order to reduce the effort required to, on the one hand, set up and operate the database and, on the other hand, to enable it to operate on Azure SQL Databases. The History Database represents only a simple data storage. The History Database does not include the One Identity Manager modules or system configuration data. There are no longer any active components.

  Declare the One Identity Manager History Database to be used for transferring data to the One Identity Manager in the TimeTrace.

  IMPORTANT:

  - It is recommended to install the History Database first!
  - Existing databases are still supported for querying archived data in TimeTrace and reports. These databases do not need to be migrated.
  - If you still want to migrate an existing History Database, ensure that the all features, procedures, tables, and views that are not in the following list are deleted by the History Database migration:

    HistoryChain, HistoryJob, ProcessChain, ProcessGroup, ProcessInfo, ProcessStep, ProcessSubstitute, RawJobHistory, RawProcess, RawProcessChain, RawProcessGroup, RawProcessStep, RawProcessSubstitute, RawWatchOperation, RawWatchProperty, SourceColumn, SourceDatabase, SourceTable, WatchOperation, WatchProperty

    Save any custom extensions before migrating.

Web Portal (API Server)

- OneLogin is used for multi-factor authentication for request and attestation approvals. Prerequisites are:
  - Synchronization with a OneLogin domain is set up and the system has been initially synchronized.
  - The value of the **ServerConfig/ITShopConfig/StepUpAuthenticationProvider** configuration key is **OneLogin MFA**.
  - In the API server's configuration file (`web.config`), the following entry must be entered in the connection string:

    ```
    <add name="OneLogin"
    ```

```
connectionString="Domain=<domain>;ClientId=<clientid>;ClientSecret=<cli
entSecret>" />
```

The respective values are taken from the OneLogin configuration.

- The request recipient must agree to the terms of use if they also act as a request approver.
- The requester is prompted to agree to the terms of use for a service item.
- A requester can request optional service items in the Web Portal.
- In the Web Portal, the historical change data of a role can be displayed in the role's overview.
- Deleted roles can now be restored in the Web Portal.
- In the Web Portal, two roles can be combined into one role. This feature is offered for departments, locations, cost centers, and business roles.
- In the Web Portal, it is possible to maintain request templates and to use them to create new requests.
- In the Web Portal, exception approvers can grant or deny approval to policy violations.
- Filters for columns and tables can be defined in the administration portal.
- Administrators and owners of applications in the Application Governance Module can have system entitlements that meet a certain condition automatically assigned to applications. Owners and administrators can be notified when their applications have been automatically assigned new system entitlements.
    - In the **QER | ITShop | MailTemplateIdents | InformAboutApplicationEntitlements** configuration parameter, you can configure the mail template to be used for mail notifications to application administrators and owners.
- In the Web Portal, request approvers can make approval recommendations. Recommendations to grant or deny requests are calculated on the basis of different criteria. The criteria are specified in the **QER | ITShop | Recommendation** configuration subparameters.

Target system connection

- Offline mode can be used to pause handling of target system-specific processes by the One Identity Manager Service if a target system cannot be reached temporarily. This prevents target system-specific processes from being frozen in the Job queue and having to be re-enabled manually later.
- Restrictions can be defined on any columns in the One Identity Manager schema when they are synchronized. For this reason, the **Synchronization information** column property is displayed in the Designer.
- Synchronization and provisioning processes are put on hold while synchronization projects are updated.

  The retry delay time is set in the **Common | Jobservice | RedoDelayMinutes** configuration parameter.

- Remote support for target system connections is implemented with .net Core resources.

  A patch with the patch ID VPR#34646_SAP is available for synchronization projects.
- Support for OneLogin as target system.

  One Identity Manager focuses on setting up and editing user accounts and providing the permissions required for accessing applications and for authentication and authorization. One Identity Manager maps the OneLogin user accounts, roles, and applications. The OneLogin connector has the task of synchronizing with OneLogin. The OneLogin API controls access to OneLogin data. OneLogin Module installation supplies synchronization templates. For more information, see the *One Identity Manager Administration Guide for Connecting to OneLogin*.
- Azure Active Directory group assignments to administrator roles are mapped in One Identity Manager.

  A patch with the patch ID VPR#33400 is available for synchronization projects.
- Rules for memberships in dynamic Azure Active Directory groups are loaded into One Identity Manager.

  A patch with the patch ID VPR#34744 is available for synchronization projects.
- The email address of Azure Active Directory user accounts can now be edited in One Identity Manager and written to the target system.

  A patch with the patch ID VPR#35286 is available for synchronization projects.
- The Azure Active Directory user accounts' creation type is loaded into One Identity Manager.

  A patch with the patch ID VPR#35290 is available for synchronization projects.
- Support for Azure Active Directory administrative units.

  A patch with the patch ID VPR#35289 is available for synchronization projects.
- Support for B2C tenants.

  A patch with the patch ID VPR#35033 is available for synchronization projects.
- Support for classifying Exchange Online Office 365 groups.

  Patches for synchronization projects with patch ID 35303_AAD and VPR#35303_O3E are provided.
- **TECH PREVIEW ONLY**: The Exchange Online connector supports certificate based authentication.

  A patch with the patch ID VPR#34766 is available for synchronization projects.

  IMPORTANT: This feature can be tested in test environments. You must definitely not use the feature in a live environment.
- Support for moving Active Directory objects across domain borders.

  A patch with the patch ID VPR#33793 is available for synchronization projects.
- Support for Microsoft Exchange mail enabled distribution groups of type **Room lists**.

  A patch with the patch ID VPR#31374 is available for synchronization projects.

- Support for Active Roles 7.5.2, Active Roles 7.5.3, and Active Roles 7.6.
- The Google Workspace connector supports synchronization of external email addresses. They can be assigned as members, owners, or managers to Google Workspace groups that allow external members.

  A patch with the patch ID VPR#34885 is available for synchronization projects.
- Support for Oracle E-Business Suite version 12.2.10.
- Support for One Identity Safeguard version 7.0.

  A patch with the patch ID VPR#35621 is available for synchronization projects.
- A new report with an overview of privileged staff access is available.
- Support for the SharePoint Server Subscription Edition.
- SAP parameters can also be inherited by SAP user accounts through system roles.

Identity and Access Governance

- Improved support for inheriting target system specific groups. It is now possible to specify for individual groups whether the manage level inheritance settings apply to the group or whether the manage level settings for the group are overwritten. For example, this can be used to specify that a group should never be removed from user accounts automatically.
- New approval policies are provided for requesting and attesting Azure Active Directory and Exchange Online system entitlements.
- The object key of the effectively assigned product is saved with the request procedure if, in the course of the approval process, the requested product is changed.
- For service items, service categories and approval steps, it can be specified whether a reason must be given or can be given optionally when requesting or making an approval decision.
- Requests can be given dynamic parameters whose values are set by the customer when they make the request. After approval, a system entitlement (`UNSGroupB`) is generated from these parameters and their values and assigned to the request recipient.
- More default objects provided for attesting employees. These attestations can be started together using a policy collection.
  - Identity itself
  - Primary or secondary departments
  - Memberships in business or system roles
  - Linked user accounts
  - Assigned system entitlements

  Approval policies can be configured to be selected when creating attestation policies in the Web Portal.

Additional approval procedures:

- CN - Challenge the decision
- PW - Owner of the attestation policy
- XM - Manager of the employee for all attestations

- Attestation policies to be run together can be combined into policy collections. A sample can be used limit the set of objects to attest for all attestation policies in the collection.
- If no report is specified on the attestation procedure, snapshots are generated containing the necessary information about the objects to be attested. The content of these snapshots can be configured.

  NOTE: The snapshot is created by the `ATT_GetAttestationObject` script. This replaces the `VI_GetAttestationObject` script.
- The date of the next attestation can be given for applications (Application Governance Module). Several default attestation policies are provided that use this date.

See also:

- Enhancements on page 8
- Resolved issues on page 14
- Schema changes on page 27
- Patches for synchronization projects on page 35

Enhancements

The following is a list of enhancements implemented in One Identity Manager 9.1.

Table 1: General

Enhancement	Issue ID
A minimum time until reactivation can be configured for DBQueue Processor tasks.	32015
The application server supports session certificates created with the CNG API.	32138
Improved performance when processing DBQueue Processor tasks.	34049
Improved error messaging if an error occurs while signing emails. Improved documentation.	35226
Changed values can be marked with an icon in the grid display. Use the display properties dialog to configure this.	35247

Enhancement	Issue ID
Improved display of the One Identity Manager Service's status page.	35285, 33313
Improved display of the application server status page.	33314
Optimized performance when evaluating conditions.	35407
The `UnitOfWork` attribute can now be used to access the currently opened Unit of Work in the scripts.	35417
Improved labeling of where-clauses as trustworthy.	35418
The **Proxy view** and **Extensions to proxy view** properties are now displayed on the **More** tab in the Schema Editor.	35613
Suuport for authentication by LDAP using an SSL connection to the LDAP server. This is configured in the **TargetSystem | LDAP | AuthenticationV2** configuration subparameters.	34453
Improved performance for generating processes.	35134, 35152
In the Designer, administrative system users can now be created in the **Getting Started** category.	35263
Improved assignment of files to machine roles.	33271
Improved behavior of the command line tools. Basic tests for parameter passing are performed. Version, error messages, and help texts are output.	35427, 34825
Improved performance determining display permissions.	35612
Improved performance when displaying processes in the Job Queue Info.	35641
The `QBM_ZDBQueueVoidTaskBulk` procedure is now supplied in addition to the `QBM_ZDBQueueVoidTask` procedure. This now allows DBQueue Processor tasks marked for bulk processing to be disabled by entering the procedure in the `QBMDBQueueTask.ProcedureName` column.	34864
It is possible to set an own query timeout at the DB session in the VI.DB, which is then used for all queries.	34917
The third-party component Microsoft.Graph has been updated.	35025
Optimization of data export from the Manager.	35349

Table 2: General web applications

Enhancement	Issue ID
In the Web Portal, the approver can see the details of the requested service items. If a role membership is requested, information about the role's	297243

Enhancement	Issue ID
permissions is displayed.	
Service items are no longer sorted on output to improve performance in Web Portal. This concerns, among other things, the service catalog and the selection of requestable products.	309523
The rule violations for a specific rule can now be viewed from an email link.	253881
Improved reports generation through the API Server.	291080
It should be possible to use the API configuration to set whether only requested entitlements and assignments are offered when requesting using a reference user or all assignments that the reference user has. In the default setting, only requested objects are shown. If exactly one request recipient is selected, this request recipient cannot be selected as a reference user.	33551, 295703
In the ImxClient command line program, the `start-update` command can be used to start a software update.	310595
Secure connection detection now supports the use of HTTPS-to-HTTP reverse proxies.	313545
The configuration of the cookie path for the CSRF protection cookie can be customized.	35620, 310602
For each entity-based API method, a restrictive filter condition can be specified in the configuration.	311030
A `MarkForDeletion()` method has been added to the `IEntity` TypeScript interface.	288697

The following ImxClient commands are changed:
`get-filestate`
`fetch-files`
`push-files`
For these commands, `/targets` is now a mandatory parameter.
	310837

Angular has been updated to version 13. This may result in the need for manual corrections to customized HTML5 code.	310627
The API Server checks the defined API routes for uniqueness at startup. A warning message is issued for non-unique routes. In the case of customized routes, warning messages may now be issued.	279209
Improved performance when listing requestable service categories in the Web Portal.	35577
The long display pattern (`DialogTable.DisplayPatternLong`) can optionally be used for displaying relationships hierarchically on forms,.	35482

Enhancement	Issue ID
The trusted source key, which can be used to specify that Where-clauses from the Web frontend are trusted, can now be specified as the `ConnectionBehaviour/TrustedSourceKey` option in the configuration file.	35239

Table 3: Target system connection

Enhancement	Issue ID
Unused virtual schema properties have been removed from the `site` mapping in Active Directory synchronization projects. A patch with the patch ID VPR#35533 is available for synchronization projects.	35533
A bug in the VPR#35343_EX0 patch has been corrected. A patch with the patch ID VPR#35506 is available for synchronization projects.	35506
The LDAP connector ignores case sensitivity when comparing values in the `ObjectClass` and `StructuralObjectClass` schema properties. A patch with the patch ID VPR#32702 is available for synchronization projects.	35702
In synchronization projects for Exchange Online and SharePoint Online, not more than one base object can be created. A patch with the patch ID VPR#30841 is available for synchronization projects.	30841
Quota settings of Exchange Online mailboxes are now synchronized. A patch with the patch ID VPR#34568 is available for synchronization projects.	34568
The mailbox permissions **Full access** and **Send as** from Exchange Online mailboxes are now synchronized. A patch with the patch ID VPR#34265 is available for synchronization projects.	34265
Improved display of app registrations and enterprise applications for Azure Active Directory in the Manager.	35212
Improved support of automatic employee assignment for guest users of Azure Active Directory user accounts.	35584
Additional revision filters are used for synchronizing SAP HCM personnel planning data. A patch with the patch ID VPR#32154 is available for synchronization projects.	32154

Enhancement	Issue ID
Improved performance in the SCIM connector. A patch with the patch ID VPR#34952 is available for synchronization projects	34952, 34953, 34954
The request timeout for querying the SCIM provider can be configured when setting up the system connection to a cloud application. A patch with the patch ID VPR#35571 is available for synchronization projects.	35571
Code snippets can be used in script variables. Examples of commonly used script variables are provided in the Synchronization Editor.	35011
Improvements to the synchronization engine. • Error handling • Detection of objects locked for synchronization • Automatic detection of synchronizations that quit unexpectedly.	35196, 35480, 35617
Improved display of additional information about the connected target system in the Synchronization Editor.	35242
The changed object is displayed in the header of provisioning logs.	35493
Improved display of the system entitlement inheritance options on the main data form for user accounts.	35524
Improved the One Identity Manager Business Application Programming Interface.	35556
Improved display of outstanding objects from assignment tables in target system synchronization.	34930
Improved display of assigned SAP groups, roles, profiles on the overview form for SAP user accounts.	34780
Improved logging of delete operations on dynamic roles.	35544
Improved performance during synchronization when a local cache is used.	34955
The following note has been included in the documentation for connecting a SAP R/3 environment with BI analysis authorizations: NOTE: BI analysis permissions are not mapped in One Identity Manager if they are indirectly assigned to SAP user accounts in SAP R/3 using SAP roles or SAP profiles. With appropriately formulated SAP functions for the S_RS_AUTH authorization object, it is still possible to check in Identity Audit whether these BI analysis authorization assignments are permitted.	35295
Improved display of inheritable groups and system entitlements on the overview forms for cloud user accounts and user accounts in custom target	35508

Enhancement	Issue ID
systems.	
The AS/400 LDAP connector has been renamed to IBM i LDAP connector.	35275
`LIKE` queries can no longer be run in the `/VIAENET/READTABLE` function module. • To apply the change, import the BAPI transport `SAPTRANSPORT_70.ZIP` into the SAP R/3 system.	35741
Improved performance processing object changes if a scope is defined.	35406
Unnecessary queries made to the SAP system when using a table-based schema extension have been omitted.	35800

Table 4: Identity and Access Governance

Enhancement	Issue ID
On the employee overview form, the client of the associated SAP user accounts is also displayed.	34929
Improved presentation of attestation case main data in the Manager.	35576
Service items can be configured as hidden in the service catalog even though they can still be requested.	35031
Completed deputizations can be deleted from the database or archived.	35096
The expiry time for adaptive maps has been increased to 24 hours. The value of the **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** configuration parameter is now **86400** by default.	35727
Completed deputizations are deleted by the DBQueue Processor once the retention period is exceeded.	35096

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 35

Resolved issues

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

Table 5: General

Resolved issue	Issue ID
Defining procedures is sporadically broken off at different stages. Error message: `Error 2021: The referenced entity 'xxx' was modified when the DDL was run. Please retry the operation.`	33544
Error running the `QBM_PJobUpdateState_Bulk` procedure: `There is insufficient system memory.`	34590
Newly issued certificates may not be accepted.	34900
In certain circumstances, mutually exclusive processes are delivered during process handling.	34973
Schedules are not sorted correctly in the Designer.	35522
Changes to the One Identity Manager Service configuration by the Job Service Configuration are not always transferred to the database.	35538
Display error in Manager on the Permissions tab in the object properties.	35558
Restore login for expired sessions in the application server does not work.	35594
Error connecting multiple Designer instances through an application server.	35668
In Manager, method definitions are displayed although the visibility permission was removed by a script.	35507
Authentication at the token endpoint using the **client_secret_post** method must include the client ID.	35691
Process steps of the `DelayComponent` process component with the `Delay` process task fail with SQL syntax errors.	35744
Application server installation fails if authentication through a system user is not allowed.	34875
New custom columns with initial values cause incorrect entries in the `QBMCustomSQL` table.	35502
Unnecessary correction of the date from **1899-12-31** to **NULL**.	35703
Issue with the automatic update under Linux.	35825
A conversion script, which is stored in the Data Import program, does not save.	35840
The Manager quits unexpectedly if more than two dependent objects are saved with the OnSaving scripts.	35838

Table 6: General web applications

Resolved issue	Issue ID
Errors occur if there are a lot of products in the Web Portal's shopping cart for which parameters must be specified.	34417
In the Web Portal, the reason stored is incorrect if products are automatically canceled due to denied attestation.	34528
When installing the Manager web application, WebView2 is installed unnecessarily.	35662
In the Web Designer preview, an error occurs when opening a service category during the request process.	35404
OAuth login to API Server fails because the `State` parameter cannot be decrypted.	35611
The display names of request items are not localized.	34865
If no matching time zone can be determined, an error message appears in the Web Designer Web Portal: `Sequence contains no matching element`.	35191
Pressing **Enter** in a date field in the Web Designer Web Portal navigates to the home page.	35559
Password questions in the Web Portal are still displayed under **Profile**, although the associated parameter has the value **false**.	35647
In the Web Portal, the product description text is not displayed in a tooltip, only the technical name.	35659
In node editing in the Web Designer, some properties do not show the data, only scroll bars.	35586
In the Password Reset Portal, after an incorrect login attempt, the authentication modules for login are displayed twice.	35546
In certain circumstances, the search in the administration portal does not return any results.	307328
When a new database session is logged in within the same API Server session, the previously used user is not logged out.	306163
The search index does not update the object keywords.	303391
The search index does not find strings containing a hyphen or a backslash in every case.	35634
When displaying attestation cases in the Web Portal, the headings of the `Grouping` and `Property` columns are not displayed correctly.	35171
Clicking on the customized company logo in the Web Portal does not open the	35658

Resolved issue	Issue ID
home page.	
In certain circumstances in the Web Portal, an error occurs opening the request history.	34893
In the Web Portal's request history, incorrect or too many groups are displayed after a search followed by grouping.	35595
An error occurs in the Web Designer if you use the **ObjectWalker** function in a column list's condition.	35782
An error occurs if a report is created in the Web Designer Web Portal when it is connected directly to the One Identity Manager database and the One Identity Manager Service that generates the report is running against an application server.	35734
Missing permissions for the session certificate in the Web Portal container.	35912

Table 7: Target system connection

Resolved issue	Issue ID
The `DPR_NeedExecuteWorkflow` script and the current `DPR_VWorkflowHandlesProperty` view do not respect the mapping direction of the mapped schema properties.	34982
A conversion error occurs when synchronizing an Active Roles domain. A patch with the patch ID VPR#35122 is available for synchronization projects.	35122
When synchronizing cloud applications with the Universal Cloud Interface connector, the `UserInGroup*` and `UserHasGroup*` tables are ignored. A patch with the patch ID VPR#35451 is available for synchronization projects.	35451
Error opening an AdminP task in the Synchronization Editor's object browser, if no database file is specified. A patch with the patch ID VPR#35500 is available for synchronization projects.	35500
When updating synchronization projects for Domino, the `MailFileAccessType` variable is not created correctly. A patch with the patch ID VPR#35745 is available for synchronization projects.	35745
Customizers prevent objects from being saved if the `XOrigin` column has the value **0**.	34854
Incorrect conversion of values in custom extensions.	35060
The display name of Azure Active Directory user accounts for guest users is not transferred to the target system.	35598

Resolved issue	Issue ID
Merge mode for the `AADApplicationOwner` and `AADServicePrincipalOwner` tables is not enabled.	35183
Azure Active Directory synchronization stops unexpectedly if an owner of a service principal is themselves a service principal. A patch with the patch ID VPR#35768 is available for synchronization projects.	35768
Microsoft Teams Teams and Microsoft Teams channels are not assigned to a scope. A patch with the patch ID VPR#35410 is available for synchronization projects.	35410
Failure to create Microsoft Teams channels.	35428
Group memberships of Active Directory groups marked for deletion are not removed.	35293
Rogue correction of Active Directory group memberships does not work.	35492
Read processes for Active Directory do not use the `OverrideVariables` parameter.	35555
Automatic employee assignment may create an unnecessary remote mailbox.	35146
The `PAG_PAGAccessOrder_CheckExistingAccessRequest` process fails.	35593
Error creating a Unix user account if the last name of the connected person contains a colon (**:**).	26374
Reloading objects in bulk mode fails if an item cannot be loaded.	34420
Conversion error synchronizing an Active Directory domain using One Identity Active Roles.	35122
If at least three processing methods are defined in a synchronization step, the order of the processing methods is swapped when the synchronization project is saved.	35499
The documentation for setting up a system connection with an Oracle Database is not up to date.	35505
When setting up the system connection with a SalesForce application, no schema types are detected.	35679
Error encrypting a database when `DPRSystemConnection.ConnectionParameter` is marked as encrypted.	35695
Single object synchronization no longer works for Azure Active Directory user accounts.	35728
The update migration of a very large database is unexpectedly stopped after 12 hours in the step `SAP 2019.0004.0017.0000 (31561)`.	35464

Resolved issue	Issue ID
When requests are generated to assign SAP roles directly to SAP user accounts, the direct assignments are deleted and recreated with a different validity period.	35648
Error applying the patch VPR#34563.	35696
The assigned system entitlements 1, 2, and 3 are not displayed on the cloud application overview form.	35512
Automatically created user accounts in custom target systems or user accounts (`UNSAccountB` table) or cloud user accounts (`CMSUser` table) do not inherit groups. For more information, see the knowledge article https://support.oneidentity.com/kb/339327.	35214
Poor performance in the Manager when displaying SAP roles that are assigned to SAP user accounts.	35761
Error updating synchronization projects with the Synchronization Editor Command Line Interface if the database is encrypted. The patches are not applied.	35805
Error deleting Azure Active Directory user account memberships in Office 365 groups.	35786
When filtering an object list, the SCIM connector ignores the date and time from the SCIM server if they are already supplied in UTC format.	35847

Table 8: Identity and Access Governance

Resolved issue	Issue ID
The permissions of the **vi_4_ITSHOPADMIN_OWNER** group for the `AADGroup` table are incorrect.	35519
Translations of an application's name are not applied to the service category.	35041
The DBQueue Processor tasks `QER-K-ShoppingRackPWOHelperPWO-Del` and `ATT-K-AttestationHelper-Del` may cause blockages.	35157
Error transporting a resource that can be requested multiple times.	35470
Lack of dependencies between DBQueue Processor tasks for allocating company resources to employees.	35294
Performance issues determining attestation objects (DBQueue Processor task `ATT-K-HelperAttestationPolicy`).	34201
Performance issues with recalculation of attestors.	35455
If an approval level with multiple approval steps is rejected due to a timeout,	35473,

Resolved issue	Issue ID
the subsequent approval level (if rejected) is not always carried out.	35474
Although an attestation case has Hold status, attestors who are redetermined for this approval step in the meantime still receive an attestation email notification. Quite rightly, the Manager and Web Portal do not display anything for these attestors to attest.	35583
Compliance checking of requests in the shopping cart and in the approval process does not detect a rule violation if it is caused by different identities of an employee. Only the cyclical compliance check detects the rule violation.	35170
Performance problems calculating groups of employees affected by compliance rules.	35261
During automatic withdrawal of entitlements after an attestation is denied, requests with the **renewal** and **cancellation** statuses are not taken into account.	34725
Immediate cancellation of a request is not possible if this request has already been previously canceled with a validity date.	35431
If the DBQueue Processor task `QER-K-ShoppingRackPWOHelperPWO` is processed in multiple slots, this task may keep getting deferred. This stops other tasks from being handled.	35466
When sending email notifications in request approval procedures, incorrect mail templates are used. Sometimes email notifications are sent even though no mail template is given in the approval step.	35496, 35819
The mail template **IT Shop request - renewal** specifies under **Requested by** the initial requester of the request, instead of the employee requesting the renewal.	35529
Requests for products for with a specified validity period can be extended indefinitely.	35651
The shopping cart cannot be filled and sent because the query that uses the `QER_FTPWOOrderPerson` function, does not finish.	35882

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 35

Known issues

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

Table 9: General known issues

Known Issue	Issue ID
Error in the Report Editor if columns are used that are defined in the Report Editor as keywords. Workaround: Create the data query as an SQL query and use aliases for the affected columns.	23521
Errors may occur if the Web Installer is started in several instances at the same time.	24198
Headers in reports saved as CSV do not contain corresponding names.	24657
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
Error connecting through an application server if the certificate's private key, used by the `VI.DB` to try and encrypt its session data, cannot be exported and the private key is therefore not available to the `VI.DB`. Solution: Mark the private key as exportable if exporting or importing the certificate.	27793
Error resolving events on a view that does not have a UID column as a primary key. Primary keys for objects in One Identity Manager always consist of one, or in the case of M:N tables, two UID columns. This is basic functionality in the system. The definition of a view that uses the `XObjectKey` as primary key, is not permitted and would result in more errors in a lot of other places. The consistency check **Table of type U or R with wrong PK definition** is provided for testing the schema.	29535
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

Table 10: Web applications

Known Issue	Issue ID
The error message `This access control list is not in canonical form and therefore cannot be modified` sometime occurs when installing the Web Portal with the Web Installer. The error occurs frequently after a Windows 10 Anniversary Update. Solution: Change the permissions for the users on the web application's parent folder (by default `C:\inetpub\wwwroot`) and apply the changes. Then revoke the changes again.	26739
In the Web Portal, a product's request properties are not transferred from the original request to the shopping cart if the request is renewed or canceled. Cause: Request properties are saved in separate custom columns. Solution: Create a template for (custom) columns in the `ShoppingCartItem` table that stores the request properties when the request is made. This template must load the request properties from the identical (custom) columns in the `PersonWantsOrg` table relating to this request.	32364
It is not possible to use the Web Designer to place a link in the header of the Web Portal next to the company name/logo.	32830
In the Web Portal, it is possible to subscribe to a report without selecting a schedule. Workaround: • 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
	33867

Known Issue	Issue ID
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> </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 11: 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 Domino connector (`Error getting revision of schema type ((Server))`). Probable cause: The HCL Domino environment was rebuilt or numerous entries have been made in the Domino Directory. Solution: Update the Domino Directory indexes manually in the HCL Domino 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.	27359

Known Issue	Issue ID
• 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.	
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 `BAPI_EMPLOYEE_GETDATA` function is always run 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
Target system synchronization does not show any information in the Manager web application. Workaround: Use Manager to run the target system synchronization.	30271
The following error occurs in One Identity Safeguard if you request access to an asset from the access request policy section and it is configured for asset-based session access of type **User Supplied**: `400: Bad Request -- 60639: A valid account must be identified in the request.` The request is denied in One Identity Manager and the error in the request is displayed as the reason.	796028, 30963
Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled. Cause: The SharePoint connector loads all object properties into cache by default. Solution: • Correct the error in the target system.	31017

Known Issue	Issue ID
- OR - • Disable the cache in the file `VI.Projector.SharePoint.<Version>.Host.exe.config`.	
If a SharePoint site collection only has read access, the server farm account cannot read the schema properties `Owner`, `SecondaryContact` and `UserCodeEnabled`. Workaround: The properties `UID_SPSUserOwner` and `UID_SPSUserOwnerSecondary` are given empty values in the One Identity Manager database. This way, no load error is written to the synchronization log.	31904

If date fields in an SAP R/3 environment contain values that are not in a valid date or time formats, the SAP connector cannot read these values because type conversion fails.
Solution: Clean up the data.
Workaround: Type conversion can be disabled. For this, SAP .Net Connector for .Net 4.0 on x64, version 3.0.15.0 or later must be installed on the synchronization server.
IMPORTANT: The solution should only be used if there is no alternative because the workaround skips date and time validation entirely.
To disable type conversion
• In the `StdioProcessor.exe.config` file, add the following settings.
• In the existing `<configSections>`:
`<sectionGroup name="SAP.Middleware.Connector">`
`<section name="GeneralSettings" type="SAP.Middleware.Connector.RfcGeneralConfiguration, sapnco, Version=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c7f7d23" />`
`</sectionGroup>`
• In the new section:
`<SAP.Middleware.Connector>`
`<GeneralSettings anyDateTimeValueAllowed="true" />`
`</SAP.Middleware.Connector>`
	32149

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

Known Issue	Issue ID
Solution: Messages in the script can be outputted using the *> operator to a file specified in the script. Example: `Write-Warning "I am a message" *> "messages.txt"` Furthermore, messages that are generated using `Write-Warning` are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an `Exception`. This message then appears in the One Identity Manager Service's log file.	
The Google Workspace connector cannot successfully transfer Google applications user data to another Google Workspace 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 Google Workspace, save a user data 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. For more information and an example XML, see *One Identity Manager Administration Guide for Connecting to Google Workspace*.	33104
In the schema type definition of a schema extension file for the SAP R/3 schema, if a `DisplayPattern` is defined that has another name in the SAP R/3 schema as in the One Identity Manager schema, performance issue may occur. Solution: Leave the `DisplayPattern` empty in the schema type definition. Then the object's distinguished name is used automatically.	33812
If target system data contains appended spaces, they go missing during synchronization in One Identity Manager. Every subsequent synchronization identifies the data changes and repeatedly writes the affected values or adds new objects if this property is part of the object matching rule. Solution: Avoid appending spaces in the target system.	33448
The process of provisioning object changes starts before the synchronization project has been updated. Solution: Reactivate the process for provisioning object changes after the `DPR_Migrate_Shell` process has been processed.	
After an update from SAP_BASIS 7.40 SP 0023 to SP 0026 or SAP_BASIS 7.50 SP 0019 to SP 0022, the SAP R/3 connector can no longer connect to the target system.	34650

Table 12: Identity and Access Governance

Known Issue	Issue ID
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
If an assignment is inherited through a role hierarchy, **bit 1** is set on the inherited assignment. Inherited assignments are consequently always indirectly assigned, even if they were originally created directly by a dynamic role or an assignment request.	35193

Table 13: Third party contributions

Known Issue	Issue ID
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

Known Issue	Issue ID
In certain circumstances, the wrong language is used in the Stimulsoft controls in the Report Editor.	31155
When connecting an external web service using the web service integration wizard, the web service supplies the data in a `WSDL` file. This data is converted into Visual Basic .NET code with the Microsoft WSDL tools. If, in code generated in this way, default data types are overwritten (for example, if the `boolean` data type is redefined), it can lead to various problems in One Identity Manager.	31998

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

Schema changes

The following provides an overview of schema changes from version 8.2.1 up to version 9.1.

OneLogin Module

- New data model for the OneLogin Module.

Configuration Module

- New columns `DialogHistoryDB.IsTransportTarget` and `DialogHistoryDB.TransportConnectionString` for archiving data in a One Identity Manager History Database.
- New column `DialogParameter.OnPropertyChangedScript` for mapping a script that runs when values change.
- New column `DialogProcessSubstitute.ReadyForDeleteOrExport` for flagging a process as completed and deleted so can be therefore be exported.
- New column `DialogTable.TransportSingleUser` to map a single user mode for transport.
- New column `DialogUser.IsDisabledForDirectLogin` for flagging whether the system user can be used for direct login.
- New columns `QBMFileHasDeployTarget.ObjectKeyDeployTarget` and `QBMFileHasDeployTarget.UID_QBMFileHasDeployTarget` for assigning files to machine roles.
- New column `QBMPwdPolicy.AdditionalPwdRequirements` for describing the additional password requirements that will be checked in the test script.
- New columns `QBMServer.IsJobServiceSuspended` and `QBMServer.SuspendReason` to stop the service when a target system goes offline.
- New mandatory field definition for the `QBMFileHasDeployTarget.XObjectKey` column.
- The following columns have been extended to `varchar(990)`.
    - DialogHistoryDB.ConnectionString
    - DialogWebService.ProxyPassword
    - DialogWebService.UserPassword
    - QBMPwdPolicy.DefaultInitialPassword
    - QBMServer.SRVAccount
    - QBMServer.SRVAccountDomain
    - QBMServer.SRVAccountPwd
- The `QBMVPwdPolicyColumns.ColumnName` and `QBMVPwdPolicyColumns.TableName` columns have been extended to `varchar(30)`.
- The `QBMVPwdPolicyColumns.UID_DialogColumn` and `QBMVPwdPolicyColumns.UID_DialogTableReference` columns have been extended to `varchar(38)`.
- The column `QBMFileHasDeployTarget.UID_QBMDeployTarget` column has been deleted.

Target System Synchronization Module

- New column `DialogColumn.SyncInfo` for mapping restrictions for synchronizing columns.
- New column `DPRAttachedDataStore.OwnerSchema` for better access to schema information.

- New columns DPRJournal.CausingEntityDisplay, DPRJournal.CausingEntityKey, and DPRJournal.JobId for improved logging.
- New column DPRStartSequenceHasProjection.CurrentJobReference for mapping the process that is currently running.
- New columns DPRRootObjConnectionInfo.IsOffline and DPRRootObjConnectionInfo.IsOfflineModeAvailable for flagging offline mode.
- The data type of the DPRShell.IsFinalized column has been changed to int.

Target System Base Module

- New table TSBSpecificGroupBehavior for overwriting the inheritance settings of groups from the manage level.
- The UNSAccountB.Password column has been extended to varchar(990).

Azure Active Directory Module

- New tables AADAdministrativeUnit, AADGroupInAdministrativeUnit, and AADUserInAdministrativeUnit for mapping Azure Active Directory administrative units.
- New table AADUserIdentity and new column AADUser.Identities for mapping identities of Azure Active Directory user accounts.
- New table AADGroupInDirectoryRole and new column AADGroup.IsAssignableToRole for assigning Azure Active Directory groups to administrator roles.
- New table AADGroupClassificationLbl for classifying Office 365 groups.
- AADOrganization.TenantType for mapping tenant types.
- New column AADUser.CreationType for mapping the creation type of Azure Active Directory user accounts.
- New columns AADGroup.MembershipProcessingState and AADGroup.MembershipRule for mapping rules for memberships in dynamic Azure Active Directory groups.
- The AADUser.Password column has been extended to varchar(990).

Exchange Online Module

- New tables O3EMailboxFullAccessPerm and O3EMailboxSendAsPerm for mapping mailbox permissions.
- New columns O3EMailbox.IssueWarningQuota, O3EMailbox.ProhibitSendQuota and O3EMailbox.ProhibitSendReceiveQuota for mapping thresholds for Exchange Online mailboxes.
- New column O3EUnifiedGroup.UID_AADGroupClassificationLbl for classifying Office 365 groups.
- The O3EMailUser.Password column has been extended to varchar(990).

Active Directory Module

- New columns `ADSDomain.AdUserName`, `ADSDomain.AdUserPassword`, and `ADSDomain.UID_ADSMachineRIDMaster` to support moving Active Directory objects across domains.
- The `ADSAccount.UserPassword` column has been extended to `varchar(990)`.

Microsoft Exchange Module

- New columns `EX0DL.RecipientType` and `EX0DL.RecipientTypeDetails` for mapping recipient types for mail-enabled distribution groups.
- The `ADSDomain.EX0UserPassword` column has been extended to `varchar(990)`.

LDAP Module

- The `LDAPAccount.UserPassword` and `LDAPContainer.UserPassword` columns have been extended to `varchar(990)`.

Oracle E-Business Suite Module

- The `EBSUser.Password` column has been extended to `varchar(990)`.

Domino Module

- The following columns have been extended to `varchar(990)`.
  - NDOCertifier.Password
  - NDOServer.Password
  - NDOUser.InternetPassword
  - NDOUser.Password
  - NDOUser.PasswordInitial

Google Workspace Module

- New tables `GAPExternalEmail` and `GAPExternalEmailInGroup` for mapping external email addresses.
- The `GAPUser.Password` column has been extended to `varchar(990)`.

SAP R/3 User Management module Module

- New column `ESetHasEntitlement.ParameterValue` for system roles to inherit SAP parameters.
- New column `SAPVSAPUserInSAPRoleAll.UID_SAPMandant` for improved displaying of roles, groups, and profiles of SAP R/3 user accounts.
- The `SAPUser.Password` column has been extended to `varchar(990)`.

Privileged Account Governance Module

- New columns to map access requests for One Identity Safeguard remote desktop session requests.
  - PAGAsset.IsRDPApplicationHostPlatform
  - PAGReqPolicy.ObjectKeyRDPAppHostAccount
  - PAGReqPolicy.RDPApplicationAlias
  - PAGReqPolicy.RDPApplicationDisplayName
  - PAGReqPolicy.UID_PAGAssetRDPAppHost
- New columns to map access requests for SSH keys for One Identity Safeguard.
  - PAGAsset.SSHHostKeyFingerPrintSha256
  - PAGReqPolicy.AllowSessionSSHKeyRelease
  - PAGReqPolicy.ChangeSSHKeyAfterCheckin
  - PAGReqPolicy.PassphraseProtectSSHKey
- New column `PAGUser.ChangePasswordAtNextLogin` for flagging whether the user must change their password the next time they log in.
- New column `PAGUsrGroup.AdminRoles` for mapping a list of permissions that all users added to the group should receive.
- New column `PAGUser.AllowPersonalAccounts` for supporting the vault for personal passwords.
- The `PAGUser.Password` column has been extended to `varchar(990)`.

Cloud Systems Management Module

- The `CSMUser.Password` column has been extended to `varchar(990)`.

Universal Cloud Interface Module

- The `UCIUser.Password` column has been extended to `varchar(990)`.

Identity Management Base Module

- New table `QERTermsOfUseHasFile` for assigning files to terms of use.
- New column `AccProduct.IsToHideFromITShop` for flagging whether the service item is hidden from the service catalog.
- New columns `PersonWantsOrg.Recommendation` and `PersonWantsOrg.RecommendationDetail` for mapping approval decision recommendations for the approver in the IT Shop.
- New column `PersonWantsOrg.ObjectKeyFinal` for mapping the effectively assigned product.

- New columns `PersonWantsOrg.UID_QERJustificationOrder` and `ShoppingCartItem.UID_QERJustificationOrder` for mapping standard reasons.
- New column `PWODecisionMethod.IsHideFromSelection` for flagging whether the approval policy is hidden in the Web Portal.
- The `Person.CentralPassword` and `Person.Passcode` columns have been extended to `varchar(990)`.
- The `PWODecisionStep.ComplianceRelevance` and `QERWorkingStep.ComplianceRelevance` columns have been deleted.

Attestation Module

- New table `AttestationPolicyGroup` and new columns `AttestationPolicy.UID_AttestationPolicyGroup` and `AttestationRun.UID_AttestationPolicyGroup` for grouping attestation policies.
- New columns `AttestationCase.Recommendation` and `AttestationCase.RecommendationDetail` for mapping approval decision recommendations for the approver in the IT Shop.
- New column `AttestationObject.ObjectReportMode` as attestation object snapshot.
- New columns `AttestationPolicy.ApproveReasonType` and `AttestationPolicy.DenyReasonType` for mapping the type of reason.
- New column `AttestationPolicy.IsSingleCaseNotification` for flagging whether notifications are always send about pending attestations.
- New column `AttestationPolicy.UID_QERTermsOfUse` for assigning terms of use.
- New column `AttestationRun.UID_AttestationPolicy` for mapping the attestation policy.

Application Governance Module

- New columns `AOBApplication.WhereClause` and `AOBApplication.WhereClauseAddOn` to define filter conditions for automatically creating application entitlements..
- New column `AOBEntitlement.IsDynamic` for flagging automatically created application entitlements.

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 8.2.1 to version 9.1. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 58.

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 35.

Table 14: Overview of synchronization templates and patches

Module	Synchronization template	Type of modification
Target System Synchronization Module	Automatic One Identity Manager synchronization	changed
Azure Active Directory Module	Azure Active Directory synchronization	changed
	Azure Active Directory B2C tenant	new
Active Directory Module	Active Directory synchronization	changed
Active Roles Module	Synchronize Active Directory domain via Active Roles	none
Cloud Systems Management Module	Universal Cloud Interface synchronization	changed
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	changed
	Oracle E-Business Suite CRM data	changed
	Oracle E-Business Suite HR data	changed
	Oracle E-Business Suite OIM data	changed
Microsoft Exchange Module	Microsoft Exchange 2013/2016/2019 synchronization (v2)	changed
	Microsoft Exchange 2010 synchronization (deprecated)	deleted
	Microsoft Exchange 2010 synchronization (v2)	deleted
Google Workspace Module	Google Workspace synchronization	changed

Module	Synchronization template	Type of modification
LDAP Module	AD LDS synchronization	changed
	AD LDS Synchronization (version 2)	changed
	OpenDJ synchronization	changed
	OpenDJ Synchronization (version 2)	changed
	Generic LDAP Synchronization (version 2)	changed
	Oracle DSEE Synchronization (version 2)	changed
Domino Module	Lotus Domino Synchronization	changed
Exchange Online Module	Exchange Online synchronization (v2)	changed
Microsoft Teams Module	Microsoft Teams (via Azure Active Directory)	changed
OneLogin Module	OneLogin Domain Synchronization	new
Privileged Account Governance Module	One Identity Safeguard synchron-ization	changed
SAP R/3 User Management module Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	none
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	none
SAP R/3 Compliance Add-on Module	SAP R/3 authorization objects	none
SAP R/3 Structural Profiles Add-on Module	SAP R/3 HCM authentication objects	changed
	SAP R/3 HCM employee objects	changed
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

Patches for the following patch types are provided in One Identity Manager 9.1.

- Patches for solved issues
- Patches for new features
- Milestones

To adjust existing synchronization projects to One Identity Manager version 9.1, you must implement milestones. A milestone is provided for each context. A milestone includes all patches for solved issues together with milestones from previous versions, if they have not already been implemented. Once the current milestone has been implemented in a synchronization project, the project is then compatible with One Identity Manager 9.1.

Patches for new features can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 9.1 for synchronization projects. Only patches created after version 8.2.1 are listed. For information about patches from earlier versions of One Identity Manager, see the respective release notes for each version.

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.

TIP: Implement milestones first and then apply optional patches for new features.

For more information, see Applying patches to synchronization projects on page 58.

Table 15: General patches

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **DPR**.	
	Milestone 9.1	Milestone for the context **One Identity Manager**.	

Table 16: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#33400	New property mapping rule for assigning administrator roles to Azure Active Directory groups	Adds a property mapping rule for the `IsAssignableToRole` schema property to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated. Dependent on the **Filter**	33400

Patch ID	Patch	Description	Issue ID
		members of directory roles patch (VPR#33399).	
VPR#34744	New property mapping rule for mapping the properties of dynamic Azure Active Directory groups	Adds property mapping rules for the `membershipRuleProcessingState` and `membershipRule` schema properties to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated.	34744
VPR#35033	Support for B2C tenants	Adds property mapping rules for the `TenantType` and `Identities` schema properties in the `Organization` and `User` mappings.	35033
VPR#35286	Allows writing of email addresses of Azure Active Directory user accounts.	Corrects the property mapping rule for the `Mail` schema property in the `User` mapping. This patch is applied automatically when One Identity Manager is updated.	35286
VPR#35289	Support for administrative units	Extends the synchronization configuration to support administrative units. This patch is applied automatically when One Identity Manager is updated.	35289
VPR#35290	New property mapping rule for the creation type of Azure Active Directory user accounts.	Adds a property mapping rule for the `CreationType` schema property to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated.	35290
VPR#35303_AAD	Supports classifications	Extends the synchronization configuration to support classification of Exchange Online Office 365 groups.	35303
VPR#35768	Corrects of the `ServicePrincipal` mapping	Corrects the property mapping rule for the `Owners` schema property in the `ServicePrincipal`	35768

Patch ID	Patch	Description	Issue ID
		mapping. This patch is applied automatically when One Identity Manager is updated. Depending on patch **Azure Active Directory service principal support** (VPR#33088).	
	Milestone 9.1	Milestone for the context **Azure Active Directory**.	

Table 17: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#35533	Removes unused schema properties	Removes unused virtual schema properties from the `site` mapping. This patch is applied automatically when One Identity Manager is updated.	35533
VPR#33793	New property mapping rule for mapping the domain's RID master	Adds a property mapping rule for the `UID_ADSMachineRIDMaster` schema property to the `domainDNS` mapping. This patch is applied automatically when One Identity Manager is updated.	33793
	Milestone 9.1	Milestone for the context **Active Directory**.	

Table 18: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#35122	Updates the target system schema	Updates the target system schema to update data types in the stored schema. This patch is applied automatically when One Identity Manager is updated.	35122
	Milestone 9.1	Milestone for the context **Active Roles**.	

Table 19: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#31374	Support for room lists	Adds property mapping rules for the `RecipientType` and `RecipientTypeDetails` schema properties to the `DistributionGroup` mapping. This patch is applied automatically when One Identity Manager is updated.	31374
VPR#35506	Corrects the behavior of "unlimited" values	Corrects the treatment of "unlimited" values. Schema properties and property mapping rules are adjusted for this. This patch is applied automatically when One Identity Manager is updated.	35506
	Milestone 9.1	Milestone for the context **Microsoft Exchange**.	

Table 20: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#30841	Prevents the creation of additional base objects	Changes synchronization project settings to prevent more than one base objects being added. This patch is applied automatically when One Identity Manager is updated.	30841
VPR#34568	New property mapping rules for mapping quota settings for mailboxes	Adds property mapping rules for the `ProhibitSendQuota`, `IssueWarningQuota` and `ProhibitSendReceiveQuota` schema properties to the `mailbox` mapping.	34568
VPR#34265	Mailbox permissions support	Extends the synchronization configuration to map the **Full Access** and **Send As** mailbox permissions. This patch is applied automatically when One Identity Manager is updated.	34265
VPR#34766	Support for certificate-based authentication	Adds the `AADOrganization` variable to the default variable set. This patch is applied automatically when One Identity Manager is updated.	34766
VPR#35343_	Supports	Extends the synchronization	35303

Patch ID	Patch	Description	Issue ID
O3E	classifications	configuration to support classification of Exchange Online Office 365 groups. This patch is applied automatically when One Identity Manager is updated.	
	Milestone 9.1	Milestone for the context **Exchange Online**.	

Table 21: Patches for Microsoft Teams

Patch ID	Patch	Description	Issue ID
VPR#35410	Updating the One Identity Manager schema	Updates the One Identity Manager schema to properly set the scope for `O3TTeam` and `O3TTeamChannel`. This patch is applied automatically when One Identity Manager is updated.	35410
	Milestone 9.1	Milestone for the context **Azure Active Directory**.	

Table 22: Patches for Google Workspace

Patch ID	Patch	Description	Issue ID
VPR#34885	Extensions for synchronizing Google Workspace external email addresses	Extends the synchronization configuration for synchronizing external email addresses	34885
	Milestone 9.1	Milestone for the context **Google Workspace**.	

Table 23: Patches for LDAP

Patch ID	Patch	Description	Issue ID
VPR#35702	Ignore upper and lower case when comparing values	Set the **Ignore case** option in the property mapping rules of the `ObjectClass` and `StructuralObjectClass` schema properties. This patch is applied automatically when One Identity Manager is updated.	35702
	Milestone 9.1	Milestone for the context **LDAP**.	

Table 24: Patches for HCL Domino

Patch ID	Patch	Description	Issue ID
VPR#35500	Correction of the `vrtProxyDataBaseName` schema property	Corrects the script for loading the `vrtProxyDataBaseName` schema property of the `AdminRequest (all)` schema class. This patch is applied automatically when One Identity Manager is updated.	35500
VPR#35745	Check value of variable `MailFileAccessType`	Checks and corrects the `MailFileAccessType` variable in all variable sets. This patch is applied automatically when One Identity Manager is updated.	35745
	Milestone 9.1	Milestone for the context **HCL Domino**.	

Table 25: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#35621	Support for One Identity Safeguard 7.0 (LTS)	Extends the synchronization configuration to support One Identity Safeguard version 7.0 (LTS).	35621
	Milestone 9.1	Milestone for the context **Privileged Account Management**.	

Table 26: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#34646_SAP	Updates the target system schema	Updates the target system schema. This patch is applied automatically when One Identity Manager is updated.	34646
	Milestone 9.1	Milestone for the context **SAP R/3**.	

Table 27: 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 **Main Identity**, **Workdates of Employee**, and **Communication Data** synchronization steps.	32154
	Milestone 9.1	Milestone for the context **SAP R/3 structural profile add-on**.	

Table 28: Patches for SAP R/3 BI analysis authorizations

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **SAP R/3 analysis authorizations add-on**.	

Table 29: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **SAP R/3**.	

Table 30: Patches for SharePoint

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **SharePoint**.	

Table 31: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#30841	Prevents the creation of additional base objects	Changes synchronization project settings to prevent more than one base objects being added. This patch is applied automatically when One Identity Manager is updated.	30841
	Milestone 9.1	Milestone for the context **SharePoint Online**.	

Table 32: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#34952	Additional certificate options for system connections	Adds new variables to the default variable set and connection parameters. This patch is applied automatically when One Identity Manager is updated.	34952
VPR#35571	New variable for configuring a request timeout	Adds a variable to configure the request timeout to the default variable set and connection parameters.	35571
	Milestone 9.1	Milestone for the context **SCIM**.	

Table 33: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)

Patch ID	Patch	Description	Issue ID
VPR#35451	Handling of `XIsInEffect columns` for all `UserInGroup*` and `UserHasGroup*` tables.	Adds special handling of the `XIsInEffect` columns for all `UserInGroup*` and `UserHasGroup*` tables to the corresponding mappings and workflows.	35451
	Milestone 9.1	Milestone for the context **Universal Cloud Interface**.	

Table 34: Patches for Unix

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **Unix**.	

Table 35: Patches for the One Identity Manager connector

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **Database**.	

Table 36: Patches for the CSV connector

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **CSV**.	

Deprecated features

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

- In future, mutual aid as well as password questions and password answers will not be supported in the Manager.

  Use the Password Reset Portal to change passwords. Save your password questions and password answers in the Web Portal.
- The SOAP Web Service is no longer supported.
- The SPML Webservice is no longer supported.
- The API Designer is no longer supported.

  Added instructions in the One Identity Manager API Development Guide on how to convert XML-based API definition code into a plugin library.
- Administration of different versions of a compiled project using compilation branches is no longer supported.
- The Visual Studio Code extension for HTML application development is no longer supported.
- Compiling HTML applications in the Database Compiler is no longer supported.
- The SharePoint 2010 connector is no longer supported.
- The Microsoft Exchange 2010 connector is no longer supported.
- The **Relevance for compliance** property for IT Shop requests (`PWODecisionStep.ComplianceRelevance` and `QERWorkingStep.ComplianceRelevance`) is no longer supported.
- Starling Two-Factor Authentication and the Starling 2FA app are no longer be supported as the Starling Two-Factor Authentication service will be discontinued on November 1, 2022.
  - OneLogin is used for multi-factor authentication for requests or attestation.
  - Use the new functionality of adaptive cards with Starling Cloud Assistant to approve requests and attestation cases.
- The generic LDAP connector is no longer supported. Use the **LDAP Connector (version 2)**.

The following features will be discontinued in later One Identity Manager versions and should no longer be utilized:

- The following script are labeled obsolete. A warning to this effect is issued during compilation.
  - VI_GetValueOfObject
  - VID_GetValueOfDialogObject
  - VI_ITDataFromOrg

- VI_AE_ITDataFromOrg
- VI_GetOrgUnitFromCertifier
- VI_ConvertDNToCanonicalName
- VI_PersonAuto_LDAP
- VI_PersonAuto_ADS
- VI_PersonAuto_EBS
- VI_PersonAuto_Notes
- VI_PersonAuto_SAP
- VI_PersonAuto_SharePoint_SPSUser
- VI_GetAttestationObject

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.*

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

Every One Identity Manager installation can be virtualized. Ensure that performance and resources are available to the respective One Identity Manager component according to system requirements. Ideally, resource assignments for the database server are fixed. Virtualization of a One Identity Manager installation should only be attempted by experts with strong knowledge of virtualization techniques.

Minimum requirements for the database server

A server must meet the following system requirements for installation of a One Identity Manager database. Depending on the number of One Identity Manager modules and the accounts managed in One Identity Manager, the requirements for working memory, hard disk storage, and processors may be significantly greater than the minimum requirements.

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 perform-

	ance.
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 2019 Standard Edition (64-bit) with the current cumulative update NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems. • Compatibility level for databases: SQL Server 2019 (150) • Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) • SQL Server Management Studio (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.

NOTE: In virtual environments, you must ensure that the VM host provides performance and resources to the database server according to system requirements. Ideally, resource assignments for the database server are fixed. Furthermore, optimal I/O performance must be provided, in particular for the database server. For more information about virtual environments, see Product Support Policies.

Minimum requirements for clients

The following system requirements must be met on the clients.

Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	1 GB
Operating system	Windows operating systems Following versions are supported: • Windows 11 (x64) • 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
Additional software	• Microsoft .NET Framework version 4.8 or later • Microsoft Edge WebView2
Supported browsers	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimum requirements for the Job server

The following system prerequisites must be fulfilled to install the One Identity Manager Service on a server.

Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2

	• Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project.
Additional software	Windows operating systems • Microsoft .NET Framework version 4.8 or later NOTE: Take the target system manufacturer's recommendations for connecting the target system into account. Linux operating system • Mono 5.14 or later

Minimum requirements for the web server

The following system prerequisites must be fulfilled to install web applications on a web server.

Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • 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 systems • Microsoft .NET Framework version 4.8 or later

- Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.8 and the 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

The following system prerequisites must be fulfilled for installation of the application server.

Processor	8 physical cores 2.5 GHz+
Memory	8 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2022 • Windows Server 2019

	• Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • 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 systems
	
	• Microsoft .NET Framework version 4.8 or later
	• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.8 and the 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 37: 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 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, Windows Server 2019 and Windows Server 2022.
Microsoft Exchange connector	• Microsoft Exchange 2013 with cumulative update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange hybrid environments
SharePoint connector	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
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

Connector	Supported data systems
	• 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.
Domino connector	• IBM Domino Server versions 8, 9, and 10 • HCL Domino Server versions 11 and 12 • IBM Notes Client 8.5.3 and 10.0 • HCL Notes Client versions 11.0.1 and 12.0 The 64-bit variant of Notes Client 12.0.1 is currently not supported.
Generic database connector	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe connector	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.5, 7.5.2, 7.5.3, and 7.6
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 (L5) • Microsoft Cloud Germany • Azure Active Directory and Microsoft 365 operated by

Connector	Supported data systems
	21Vianet in China For more information, see https://support.oneidentity.com/KB/312379. • Microsoft Teams
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
Google Workspace connector	• Google Workspace
Oracle E-Business Suite connector	• Oracle E-Business Suite versions 12.1, 12.2, and 12.2.10
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard versions 6.0, 6.7, 6.13, and 7.0

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

IMPORTANT: Note the Advice for updating One Identity Manager on page 53.

Advice for updating One Identity Manager

- One Identity Manager 9.1 is a further development of version 8.2.1. All official releases of version 9.0 without cumulative updates, 8.2.1, 8.1.5 or older can be upgraded to version 9.1. Updating newer versions can lead to a downgrade.
- Test changes in a test system before you load a migration package into a production system. Use a copy of the production database for testing.
- 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 9.1. Otherwise the schema update cannot be completed successfully.
- For One Identity Manager databases on SQL Servers, it is recommended, on performance grounds, that you set the database to the **Simple** recovery model for the duration of the schema update.
- During the update of a One Identity Manager database version 8.0.x to version 9.1, 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\MSSQL2K\30374.sql`) is provided. In case it fails, correct the data and restart the update.
- 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, calculation tasks are queued in the database. These are processed by the DBQueue Processor. Processing calculation tasks may take some time depending on the amount of data and system performance.

  This is particularly the case if you save large amounts of historical data in the One Identity Manager database, such as change data or data from process handling.

  Therefore, ensure that you have configured an appropriate procedure for archiving the data before you update the database. For more information about archiving data, see the *One Identity Manager Data Archiving Administration Guide*.
- For the period of the update, the database is set to single user mode. Close all existing connections to the database before starting the schema update.
- You may experience problems activating single-user mode when using database mirroring.
- During installation of a new One Identity Manager database with version 9.1 or while updating a One Identity Manager database from version 8.0.x to version 9.1, 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.

  > NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.1, 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, 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.
- After the update has completed, the database switches automatically to multi-user mode. If this is not possible, you receive a message in which you can manually switch to multi-user mode.
- 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 9.1

IMPORTANT: Note the Advice for updating One Identity Manager on page 53.

To update an existing One Identity Manager installation to version 9.1

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

      All the database tests must be successful. Correct any errors. Some consistency checks offer repair options for correcting errors.
2. Update the administrative workstation, on which the One Identity Manager database schema update is started.
   a. Run the `autorun.exe` program 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 Active Directory Edition, switch to the **Other Products** tab and select the **One Identity Manager Active Directory Edition** entry.

   c. Click **Install**.

      This starts the installation wizard.
   d. Follow the installation instructions.

      IMPORTANT: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.
3. Complete 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 the **150** and change it if necessary.
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 8.0.x to version 9.1, 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, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

7. Update the One Identity Manager Service on the update server.
   a. Run the `autorun.exe` program from the root directory on the One Identity Manager installation medium.
   b. Change to the **Installation** tab. Select the Edition you have installed.
      - To update a One Identity Manager Active Directory Edition, switch to the **Other Products** tab and select the **One Identity Manager Active Directory Edition** entry.
   c. Click **Install**.

      This starts the installation wizard.
   d. Follow the installation instructions.

      IMPORTANT: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.
8. Check the login information of the One Identity Manager Service. Specify 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 9.1

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 run the process, the One Identity Manager Service must be started on all synchronization servers.

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

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

   For more information, see Applying patches to synchronization projects on page 58.

To update an application server to version 9.1

- 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 Designer Web Portal to version 9.1

NOTE: Ensure that the application server is updated before you update the Web Designer Web Portal.

- To update the Web Designer 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 Designer Web Portal, uninstall the existing Web Designer Web Portal installation and reinstall the Web Designer Web Portal. For more instructions, see the *One Identity Manager Installation Guide*.

To update an API Server to version 9.1

- 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 9.1

- (As from version 8.1.x) After updating the API Server, the Operations Support Web Portal is also current.
- (As from version 8.0.x)

1. Uninstall the Operations Support Web Portal.
2. Install an API Server. For more instructions, see the *One Identity Manager Installation Guide*.

To update the Manager web application to version 9.1

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. (Optional) 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 milestone you want to implement.

   In **Details - Installation summary**, all dependent patches are displayed in order of installation.
4. Click **Apply selected patches**.

5. Enter any user input as prompted.
6. (Optional) In **Available patches**, select the patches for new features that you want to apply. Multi-select is possible.

   In **Details - Installation summary**, all patches are displayed in order of installation.

   a. Click **Apply selected patches**.

   b. Enter any user input as prompted.
7. Use the patch log to check whether customization need to be reworked.
8. If required, rework customizations in the synchronization configuration.
9. Run a consistency check.
10. Simulate the synchronization.
11. (Optional) Activate the synchronization project.
12. 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 33
- Patches for synchronization projects on page 35

Verifying successful installation

To determine if this version is installed

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

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

  The version number 2022.0009.0001.0000 for all modules and the application version 9.1 v91-173803 indicate that this version is installed.

Additional resources

Additional information is available from the following:

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

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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