One Identity Manager 8.2.1

Release Notes

29 April 2022, 10:34

These release notes provide information about the One Identity Manager release, version 8.2.1. You will find all the modifications since One Identity Manager version 8.2 listed here.

One Identity Manager 8.2.1 is a patch release with new functionality and improved behavior. See New features on page 2 and Enhancements on page 5.

If you are updating a One Identity Manager version older than One Identity Manager 8.2, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under One Identity Manager Support.

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

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

For the most recent version of the product information, see the One Identity Manager documentation.

About One Identity Manager 8.2.1

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 concern with One Identity Manager

Each one of these scenario specific products is based on an automation-optimized architecture that addresses major identity and access management challenges at a fraction of the complexity, time, or expense of "traditional" solutions.

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 cloud.oneidentity.com.

New features

New features in One Identity Manager 8.2.1:

General

- Processing of the internal DBQueue Processor requests can be carried out 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.

  If you use the Configuration Wizard to install or update the database, you can select whether to use the Database Agent Service or the SQL Server Agent for processing internal tasks in the database. The system configuration overview shows you which Agent is in use.

  > IMPORTANT: This is an EXPERIMENTAL function. The performance impact on production systems has not been determined. Therefore this feature is not yet

covered by support. However, you are welcome to try it (preferably in non-production systems) and if you have any feedback, send it to OneIM.Beta@oneidentity.com.

- Querying secrets in process step parameters is supported. Syntax: `&SECRET(Name)&`

  In the One Identity Manager Service configuration, secrets that are allowed to be used as replacements are given in the `SecretsAllowList` parameter. The `SecretsFolder` parameter specifies the directory where the secrets files are located.
- Querying environment variable in process step parameters is supported. Syntax: `&ENV(variable name)&`
- In the One Identity Manager Service configuration, HTTP headers for the status page can be configured in the `HTTPHeaders` parameter.
- The command line program `DBConsCheckCmd.exe` is deployed for running consistency checks.
- To stop properties from being edited, users require the **Allows a change lock to be set for specified properties of individual objects** program function (`Common_AllowPropertyLocks`).

  If certain users are supposed to be able to lock properties for editing, you can assign the permissions to the users through permissions groups. The **QBM_PropertyLock** permissions group is provided for non-role based login. For role-based logon, the **Basic Roles | Lock single properties** application role is provided.

Web applications

- Changed the heuristics for detecting the time zone to use browser standards.
- Added a code sample that shows how to integrate a multi-factor authentication provider for session authentication.
- It is now possible to upload and host custom versions of standard HTML applications (for example, the Web Portal).
- For HTML applications, it is possible to convert local changes to global changes using a configuration in the Administration Portal.
- In the Administration Portal you can define your own logo for the Web Portal.
- In the Password Reset Portal, it is now possible to register as a new user or create a new user account.
- In the Operations Support Web Portal, it is now possible to display the number of processes per queue in a table as well as in a diagram.
- Provisioning processes can be handled manually in the Operations Support Web Portal.
- It is now possible to display additional columns and information in tables in the Web Portal (configurable in the Administration Portal).
- Dynamic roles for memberships can be configured in the Web Portal.
- In the Web Portal, it is now possible to manage request templates and use them for requests. You can create your own request templates.

- In the Web Portal, owners can be assigned to devices. It is possible to claim ownerships of devices.
- In the Web Portal, it is now possible to create new identities.
- The history of an identity can be displayed in the Web Portal.
- In the Web Portal, it is now possible to display rule violations and grant or deny exceptions.
- The Web Portal can now display compliance rules.
- In the Web Portal, it is now possible to request new SharePoint groups.
- In the Web Portal, reports can now be managed (created, edited, deleted).
- New functions in the Web Portal for locations, departments, cost centers, application roles, business roles, and system roles.
    - Rule violations can be displayed for locations, departments, cost centers, application roles, business roles, and system roles.
    - Departments, locations, cost centers, business roles, system roles can be split in the Web Portal.
    - It is possible to compare departments, locations, cost centers, business roles, and system roles.
- The Web Portal shows which entitlements are lost if an attestation case is denied.
- In the Web Portal, it is now possible to escalate attestation cases and request approvals.
- In the Web Portal, pending requests that must be approved by others can be displayed on a tile on the home page.
- In the Web Portal, it is now possible to delete the complete saved for later list.

Target system connection

- Support for One Identity Active Roles version 7.5.
- The Microsoft Exchange connector has read and write access to the attribute extensions (`CustomAttibute 1` to `CustomAttibute 15`) for mailboxes, mail users, mail contacts, distribution groups, and dynamic distribution groups. To use the functionality, alter the mapping.
- It is possible to prioritize data if the connector detects conflicts between database and target system when synchronizing with the One Identity Manager database.
- If One Identity Safeguard is used for password management, sample scripts can now be used.
- In the Synchronization Editor code snippets are provided that you can use as templates for reading a system user's password from an external password management system. These code snippets can be utilized when One Identity Safeguard is implemented for password management. The code snippets can be selected and customized when creating script variables.

- The Azure Active Directory connector can load the `creationType` schema property of the `User` schema type. To use the functionality, alter the mapping.

Identity and Access Governance

- Request and attestation case approvals using Starling Cloud Assistant.

  Adaptive cards can be used to allow approvers and attestors who temporarily do not have access to their One Identity Manager tools to approve requests and attest cases. Starling Cloud Assistant transfers the adaptive cards to the approvers and attestors, waits for their response, and sends the response to One Identity Manager. In Starling Cloud Assistant, transmission channels are configured and can be set separately for each recipient. Currently, Slack, or Microsoft Teams can be used.

  For adaptive card approvals and attestations, the approval steps, service items, or service categories specify whether a reason must be provided with the approval.

  Adaptive cards replace the Starling 2FA app approval. There is still support in the Starling 2FA app in version 8.2.1 for request approvals, but it is not enabled. The Starling 2FA app will be completely removed with the next One Identity Manager release. For more information, see Deprecated features on page 42.
- Certification of new business roles, organizations, and application roles.

  The attestation functionality allows the main data of business roles, organizations, and application roles newly created in One Identity Manager to be attested and certified by its managers. The initial certification status is set by the **QER | Attestation | <...> | InitialApprovalState** configuration parameters. For roles with the **New** certification status, attestation is started and the certification status is updated according to the result.

See also:

- Enhancements on page 5
- Resolved issues on page 11
- Schema changes on page 26
- Patches for synchronization projects on page 29

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.2.1.

Table 1: General

Enhancement	Issue ID
The **Can unsubscribe** option (`DialogRichMail.AllowUnsubscribe`) can be customized for default templates.	34925

Enhancement	Issue ID
In the Job Queue Info, improved display of the change information for the `CausingEntityPatch` parameter. This parameter contains the patch that contains the changes to be provisioned.	34969
In the Job Queue Info, if an error occurs when the status is queried it is now shown. A detailed error message is displayed in the context menu.	35324
The documentation can now be displayed in the Launchpad.	34994
Improved permissions for the **QBM_BaseRight** permissions group.	35048
The information about public holidays has been updated.	35063
Altered bit positions of an assignment origin (`XOrigin` column) for assignment tables. The bit position **2** for assignments through a dynamic role has been removed.	35193, 35203, 35206
Kerberos support for HTTP authentication on the Job server.	35377
Improved performance of bulk processing DBQueue Processor tasks with large amounts of data.	34690
Improved performance when runtime plans are recompiled for the DBQueue Processor.	34803, 34813
Improved security settings for documentation.	35225
Improved testing to prevent blind SQL injections.	35166
Improved security for logging login attempts.	35230
The third-party component `DevExpress` has been updated.	35296

For security reasons, the HTML front-end of the application server can be disabled. To do this, add the following entry to the configuration file in the `<server>` section.
`<!-- Do not provide the HTML/JS frontend -->`
`<add key="nofrontend" value="true" />`
This also means that the API documentation in the application server, including the test options, is no longer available.
	35345

For security reasons, the HTML front-end of the One Identity Manager Service can be disabled. To do this, enter the IP address of the Localhost (127.0.0.1) in the `HTTP server IP address` parameter.	35345
The application server displays a **406 Not Acceptable** error message if the requested content type is not supported.	35314
The **QER | Person | PasswordResetAuthenticator | SearchColumn** configuration parameter has been extended so it is now possible to specify multiple columns. The columns can be delimited with a pipe (**|**).	34116

Table 2: Web applications

Enhancement	Issue ID
The Web Portal checks whether compliance rules can be violated by requesting an assignment to business roles or organizations, even if no employee is directly affected. This check can now be disabled.	35163
In the Operations Support Web Portal, the display of processes and filtering options has been improved.	293072
Applications can now be deleted in the Web Portal.	261577
The Web Portal displays details of products such as keywords, description, permission type, and inherited permissions.	279436
In the Web Portal, it is now possible to view reports directly in the browser.	293386
The Web Portal now displays compliance violations in the request history.	294063
The Web Portal now makes it possible to add additional reports, account definitions, and disabled Azure Active Directory service plans to a shop's shelf.	294072
Requesting for other identities in the Web Portal has been revised.	294912, 30104
The Web Portal can filter user accounts and system entitlements by target system and container.	296472
The Web Portal displays rule violations for attestation cases.	297245
The Web Portal now makes it possible to view additional information such as memberships, rule violations, reports, and assignment analysis.	298169
Improved Web Portal performance.	31057
The contents of the **Attestation of my permissions** tile on the Web Designer Web Portals home page have been improved.	30350
In the Web Designer Web Portal, no more empty directories are displayed in the main data of roles.	35066
Applications must now authenticate themselves with a special key (`Trusted Source Key`). During the initial installation, the trusted source key is configured automatically. After upgrading the One Identity Manager to version 8.2.1, you must actively configure the trusted source key. ***To configure the trusted source key*** 1. On the server where the web application is installed, open a command line utility with administrator privileges. 2. Change to a directory with installed One Identity Manager development	301102

Enhancement	Issue ID

tools.
3. Call the following command:
`imxclient edit-config /path <web.config file path> -T`
(for example `imxclient edit-config /path c:\inetpub\wwroot\apiserver\web.config -T`)
or
`imxclient edit-config /path <web.config file path> /trustedsourcekey <Key>`	

In the Administration Portal, you can now configure whether only products that have already been requested within the peer group are displayed when a request is made through a peer group.	295703
In the Administration Portal, the use of the Auth Token can now be disabled in the configuration.	301952, 35271
Security for StsSetup has been increased.	300583
The RSTS was updated to version 2022-03-30.1.	305080
Transfer of log entries from the web client to the server can now be disabled. To do this, add the following entry to the `web.config` file under `<appSettings>`: `<add key="DisableClientLog" value="true" />`	34937

Table 3: Target system connection

Enhancement	Issue ID
The time the synchronization finished is recorded in the synchronization log.	34841
The password of the synchronization user for synchronizing Oracle E-Business Suite is stored as a variable and can be encrypted separately on an encrypted database. A patch with the patch ID VPR#34775 is available for synchronization projects.	34775
A list of SAP user accounts that cannot be edited in One Identity Manager has been added to the *One Identity Manager Administration Guide for Connecting to SAP R/3*.	35331
Improved support for synchronizing child systems of a CUA that are not in the same SAP system as the central system. A patch for synchronization projects with patch ID VPR#35118 is provided.	35118
Improved support for dynamic groups in Azure Active Directory.	34777
Improved mapping of the recipient type of an Exchange Online mail user.	34938

Enhancement	Issue ID
A patch for synchronization projects with patch ID VPR#34938 is provided.	
The Active Roles connector can use the One Identity Manager Service's user account to log in on the target system. To do this, the **Use current credentials (current user/service account)** option is ensbled on the **Credentials** page in the project wizard.	34391
Improved support for the Microsoft Exchange mailbox permissions **Send As** and **Full Access**. A patch for synchronization projects with patch ID VPR#21073_2 is provided.	21073
Improved email address uniqueness checking for remote mailboxes.	35080
On the overview forms of LDAP user accounts, LDAP groups, and LDAP computers, the domain is also displayed.	34483
When automatically requesting Exchange Online mail-enabled distribution groups, the members of a group of administrators are now also used as product owners.	34850
When deleting Exchange Online mail-enabled distribution groups and Office 365 groups, as well as when deleting group memberships, the associated Azure Active Directory objects are also deleted.	34855
Improved object search in the target system during provisioning.	34184
The Synchronization Editor can display additional information about the connected target system.	33482
New synchronization projects cannot be set up nor system connections created for connectors marked as obsolete.	34479
System objects in system connectors now use less base memory.	35032
Improvements in the dialog for editing schema properties in the Synchronization Editor.	35252
The `DPR_Migrate_Shell` process has been given a higher priority to complete before any synchronization or provisioning processes start.	34903
Error provisioning a Google Workspace environment are caught when changing assignments of products and SKUs to user accounts, changing only the license but leaving the product identical.	32276
Support for SAP S/4HANA also with SAP BASIS version 7.53.	35279
Improved documentation of the permissions required for synchronizing with Oracle E-Business Suite.	34119
When using the `/VIAENET/READTABLE` function module, the table access permissions can now also be defined using the S_TABU_NAM or S_TABU_DIS authorization objects. These are tested equally.	35465

Table 4: Identity and Access Governance

Enhancement	Issue ID
Improved performance in determining the origin of employees' entitlements.	34768
Request parameters are archived when deleting completed request procedures.	33647
Improved presentation of attestation guidelines' main data.	34924
If it takes longer than 48 hours to generate new attestation cases, the process is canceled. The timeout for generating attestation cases can be set in the **QER | Attestation | PrepareAttestationTimeout** configuration parameter.	34932
Improved documentation for suspending attestations, for example, by disabling attestation policies.	34945
Samples can now only be processed in the Attestation category in the Manager.	35108
Improved display of request property and request parameter assignments to service items and service categories in the Manager.	35148
The Manager displays potential rule violations better on user interface forms. The form element for assignments that can potentially lead to rule violations has been renamed.	35147
After importing HR data, templates are run on various Person table columns only if the data was not changed by the import.	34842
Improved **Missing default entries in QERRiskIndex** consistency check.	35411
For the `PersonHasQERResource` table, assign by event (`IsAssignmentWithEvent`) is now enabled by default.	35452

See also:

- Schema changes on page 26
- Patches for synchronization projects on page 29

Resolved issues

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

Table 5: General

Resolved issue	Issue ID
Performance issues checking unique groups when adding objects.	34830
The One Identity Manager Service does not notice changes to the service account option for its system users (`DialogUser.IsServiceAccount` column).	34858
Transfer from the DBQueue buffer (`QBMDBQueuePond` table) to the DBQueue fails because in-memory tables are too large.	34867
In certain circumstances, an error occurs when calculating table statistics.	34888
Repairing the search index on the application server might not work.	34894
The One Identity Manager Service cannot be initialized if there are inconsistent processes in the Job queue. By resolving this issue, inconsistent processes are recorded in the process history.	34897
Error determining display values in simple list reports.	34923
Error opening the process information in the Manager if the program is connected through the application server.	34942
On the status page, the application server always shows the value **-1** for the software revision.	34988
In the Configuration Wizard, on the **Configure vendor notification** page, the **Back** button is active.	34989
Error running multiple data archives simultaneously. Error message: `The instance of the SQL Server Database Engine cannot obtain a LOCK resource at this time. Rerun your statement when there are fewer active users.`	35016
Incorrect **maximum degree of parallelism (DB)** value in the system configuration overview.	35022
If the `DialogDatabase.ConnectionString` column is labeled with the **Blob (external)** (`isBlobExternal = 1`) option, generating any process fails. Error message: `Value ConnectionString was not found.`	35043
If an SQL Server with version 2019 is used, the basic settings for the database are not enabled.	35084
Performance issues calculating the sort order of DBQueue Processor tasks.	35087

Resolved issue	Issue ID
If the processing state of a process step is updated, the modification date is not adjusted.	35095
Performance issues using the overload protection mechanism during bulk processing of DBQueue Processor tasks.	35103
Performance issues calculating a very large number of group memberships.	35104
Process history entries are deleted or moved to History Database too early.	35136
The object key (`XObjectKey` column) for the **Canton** time zone is incorrect.	35150
During migration, bitmasks of custom columns are not transferred to the `QBMColumnBitMaskConfig` table.	35159
Parameters without values are ignored when generating processes.	35173
Error saving deferred operations when the data contains line breaks.	35204
Importing files with placeholders in subdirectories does not work in the `SoftwareLoaderCMD.exe` command line program.	35299
When importing data using an import script in Data Import, dates and times may be changed.	35312
Migration to version 8.2 fails if a lot of UIDs have been changed.	35336, 35030
Enabling the **Log changes** (`IsToWatch` column) option on a `timestamp` column causes the generation of *Watch triggers to fail.	35384
The `VI.Projector.ScriptSupport.dll` file is not installed on the Job server.	34951
Saving a dependent object in the `OnSaved` script causes an error.	35446
In certain circumstances, the wrong translation is displayed for a value.	35436
Error encrypting a database when the password in a target system connection contains double quotes.	35408

Table 6: Web applications

Resolved issue	Issue ID
Certain special characters in the database password cause issues when installing the Web Designer Web Portal.	34294
In the Web Designer Web Portal, you cannot use a date in the filter wizard.	34435
The counter for filtered results is inaccurate if the results go over several pages. Paging is no longer available after filtering.	34506
The labels for the grouping columns and properties of attestation cases are not	34593

Resolved issue	Issue ID
displayed correctly in the Web Designer Web Portal on the **My Attestation Status** page.	
In the Web Designer, the **Maximum file size** property cannot be used for components that are to upload files.	34840
In the Web Designer Web Portal, the department IDs are displayed in the menu instead of department names.	34943
In the Web Designer Web Portal, an error occurs when editing a page's layout settings.	34983
Custom files are stored in the wrong directory when an API Server is installed.	35050
In the Web Designer Web Portal, you cannot select any objects in the address book's filter wizard.	35052
In the Web Designer Web Portal and the Web Portal it is not possible to search for products/service items with a colon in the name.	35100, 35309
In the Web Portal, data is not correctly restricted following a previous restriction. For example, after selecting a department, identities are displayed that do not belong to the selected department.	35124
In the Web Designer Web Portal, manually entering a page number in tables does not switch to the given page, but generates an error instead.	35257
When you create an Angular workspace in child folders, the HTML application can no longer be compiled.	35272
In the English language Web Designer Web Portal and in the Web Portal the search for products/service items does not work correctly.	35310
In the Web Designer Web Portal, under certain circumstances, an error occurs when displaying pending attestations.	35323

Table 7: Target system connection

Resolved issue	Issue ID
Memberships of Azure Active Directory groups that are synchronized with the local Active Directory (column `OnPremisesSyncEnabled=True`) must not be provisioned.	34448
In certain circumstances, the customizer for the `AADUserInGroup` table prevents a membership from being deleted.	34702
Error finding the user login name for Azure Active Directory user accounts in federations. A patch for synchronization projects with patch ID VPR#34896 is provided.	34896

Resolved issue	Issue ID
In certain circumstances, synchronizing with Azure Active Directory causes memberships to be marked as outstanding. The next synchronization removes the marks.	35400
Incorrectly specified processing methods in the **Calendar Processing** and **Mailbox Statistics** synchronization steps in synchronization workflows for Exchange Online. A patch for synchronization projects with patch ID VPR#35373 is provided.	35373
Some properties of Exchange Online objects, such as limits, do not distinguish between the **0** and the **unlimited** setting. By resolving this issue, the value **-1** is interpreted as **unlimited**. A patch for synchronization projects with patch ID VPR#35343_O3E is provided.	35343
Error provisioning SAP user accounts when a proxy is assigned to the user account. Patches for synchronization projects with patch ID VPR#35370 and VPR#35370_CUA are provided.	35370
Sporadic data errors in external schema extensions based on SAP tables. Data is mixed between the selected data sets.	34382
The valid until date and the **Excluded** option on existing assignments of structural profiles to SAP user accounts cannot be changed. Patches with the patch IDs VPR#35174_1 and VPR#35174_2 are available for synchronization projects.	35174
Error provisioning the `authOrig` properties of the `group` schema class in Active Directory.	34931
During synchronization of Active Directory user accounts, entries are created in the `QBMServer` table even though the **TargetSystem | ADS | AutoCreateServers** configuration parameter is not set.	34990
The `ADS_PersonUpdate_ADSAccount` script assign a state to an employee even though the Active Directory user account does not have one.	35101
The `vrtparentDN` property of Active Directory objects is formatted incorrectly if the distinguished name of the parent object contains a slash (**/**).	35458
Some properties of Microsoft Exchange objects, such as limits, do not distinguish between the **0** and the **unlimited** setting. By resolving this issue, the value **-1** is interpreted as **unlimited**. A patch for synchronization projects with patch ID VPR#35343_EX0 is provided.	35343

Resolved issue	Issue ID
Retrieving a password from One Identity Safeguard fails with an error message.	35429
Error loading objects from a cloud application using the SCIM connector.	34999
Objects that were ignored during synchronization because there were still processes for them in the Job queue, are still not processed during subsequent synchronization with revision filtering.	35049
If synchronization runs for several days but the time specified in the **DPR | Journal | LifeTime** configuration parameter is shorter, the synchronization log for the current synchronization is deleted. The synchronization quits with an error.	35135
Error synchronizing if a custom processing method runs in a synchronizations step.	35264
Unknown schema types are not displayed in the single object view of the Domino connector's target system browser.	35001
If a Notes group is renamed, the wrong name is written to the AdminP request document.	35021
Data type error reading very large amounts of data with the Domino connector.	35268
If a fixed parameter is passed to a function in a SAP schema extension file, the result list is not restricted to the parameter value.	34948
Missing synchronization user permissions for synchronizing with a SAP S/4HANA 2.0 environment.	34967
Missing permissions on the `SAPUserMandant` table in the password reset portal.	34986
The `SAPUser.Pname` column's template is only run for new objects.	35083
Locking an SAPUser of a CUA leads to a template inconsistency for SAPUser.U_Flag When locking an SAP user account in a central user administration, an incorrect value is set for the lock flag (`SAPUser.U_Flag`).	35156
Performance issues in DBQueue Processor when processing enterprise resource assignments for employees associated with SAP user accounts.	35223
`TempUserPassword` is not encrypted on the `OverrideVariables` parameter in the `SAP_SAPUser_Insert` and `SAP_SAPUser_Update` processes.	35307
Scrolling back in the System Connection Wizard for the Windows PowerShell connector mixes up settings that have already been entered.	35129
Error message opening a custom target system group in the Manager web	35187

Resolved issue	Issue ID
application.	
In the Manager web application, columns of a schema extension for a customer target system do not display the alternative column caption.	35284
It is possible to assigned account definitions to user accounts that are marked as outstanding. In certain circumstances, there is an attempt to create another user account. After solving this issue, appropriate messages are written to the log and the process could change to the **frozen** status. Rework the user account in the target system synchronization and run the whole process again.	35346
In the Synchronization Editor, tables are suggested for compression, that cannot be compressed.	35397
The CSV connector does not convert the **DateTime** value to UTC.	33676
Error displaying One Identity Manager objects in the target system browser when connecting to the One Identity Manager database using the **RemoteConnectPlugin**.	35441
Syntax errors importing One Identity Manager BAPI transports. A new BAPI transport is provided (`SAPBusinesspartnerProxies.zip`), which contains the functions defined in the /VIAENET/HELPER package. The transport is only required if a SAP S/4HANA system is connected and business partner data associated with SAP user accounts is mapped.	34976

Table 8: Identity and Access Governance

Resolved issue	Issue ID
In certain circumstances, when an Active Directory group is assigned to a shelf, several product nodes are created.	34552
In an approval level with multiple approval steps, if one of the steps is escalated, the attestation history sometimes shows the wrong approval step as escalated.	34570
When renewing or unsubscribing a request with a limited validity period, the time to unsubscribe a product is not correctly determined in UTC time.	34619
Employees who have delegated approval of attestation cases to another person are still informed that attestation cases are available for approval.	34695
In certain circumstances, the object key of a cart item (`ShoppingCartItem.ObjectKeyOrdered`) is not filled correctly.	34801
It is not possible to select a role (`ObjectKeyOfAssignedOrg`) in approval steps of custom approvals.	34805

Resolved issue	Issue ID
If several products for which request exist are moved to another shelf, some requests are canceled even though **Retain service item assignment on relocation** is set for all service items.	34914
Memberships in business roles can be requested even if the associated service item is marked as not requestable.	34934
The Analyzer does not recognize the **ApplicationStart_Analyzer** function.	34935
Automatic approvals through `ReuseDecision` may get stuck in an endless loop.	35003
Write error in the **IT Shop - approval by mail** and **Attestation - approval by mail** mail templates.	35029
Performance problems recalculating customer nodes in the IT Shop.	35117, 35302, 35357
For assignment orders, the object key of the assignment is not determined if the object key of the requested product does not exist.	35121
Performance issues calculating company policies if a large number of objects are affected.	35139
The **Objectkey references to non existing object** consistency check identifies request items of assignment request as incorrect.	35143
Error creating a report for an attestation object in the attestation case if the attestation object has a lot of recursively accessible, dependent objects.	35254
The **Overview with roles and user accounts (incl.history)** report is incomplete.	35366
In certain circumstances, if an approval step is automatically denied due to a timeout, the subsequent approval step is not run.	35440, 35454
When recalculating SAP role assignments to user accounts, the valid until date is incorrectly calculated if the assignment was created by an assignment request and the requester was deleted.	35434

See also:

- Schema changes on page 26
- Patches for synchronization projects on page 29

Known issues

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

Table 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
In certain circumstances, objects can be in an inconsistent state after simulation in the Manager. If an object is changed or saved during simulation and the simulation is finished, the object remains in the final simulated state. It may not be possible to save other modifications to this object instance. Solution: Reload the object after completing simulation.	12753
Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation. Cause: The Configuration Wizard was started directly. Solution: Always use `autorun.exe` for installing One Identity Manager components. This ensures that you do not select any invalid modules.	25315
Schema extensions on a database view of type **View** (for example `Department`) with a foreign key relation to a base table column (for example `BaseTree`) or a database view of type **View** are not permitted.	27203
Error connecting through an application server 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	30972

Known Issue	Issue ID
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`.	
If no date is given, the date 12/30/1899 is used internally. Take this into account when values are compared, for example, when used in reports. For detailed information about displaying dates and time, see the *One Identity Manager Configuration Guide*.	31322
The following error occurred installing the database under SQL Server 2019: `QBM_PDBQueueProcess_Main unlimited is only allowed as an agent job` Solution: • The cumulative update 2 for SQL Server 2019 is not supported. For more information, see https://support.oneidentity.com/KB/315001.	32814

Table 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	32938

Known Issue	Issue ID
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**.	
If the application is supplemented with custom DLL files, an incorrect version of the `Newtonsoft.Json.dll` file might be loaded. This can cause the following error when running the application: `System.InvalidOperationException: Method may only be called on a Type for which Type.IsGenericParameter is true.` `at System.RuntimeType.get_DeclaringMethod()` There are two possible solutions to the problem: • The custom DLLs are compiled against the same version of the `Newtonsoft.Json.dll` to resolve the version conflict. • Define a rerouting of the assembly in the corresponding configuration file (for example, `web.config`). Example: `<assemblyBinding > <dependentAssembly> <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30AD4FE6B2A6AEED" culture="neutral"/> <bindingRedirect oldVersion="0.0.0.0-11.0.0.0" newVersion="11.0.0.0"/> </dependentAssembly> </assemblyBinding>`	33867
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.	25401

Known Issue	Issue ID
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.	
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. • Add a custom column to the table `SAPUser`. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required.	27359
Synchronization projects for SAP R/3 that were imported by a transport into a One Identity Manager database, cannot be opened. The problem only occurs if an SAP R/3 synchronization project was not added in the target database before importing the transport package. Solution: Create and save at least one SAP R/3 synchronization project before you import SAP R/3 synchronization projects into this database with the Database Transporter.	27687
Error 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	29556

Known Issue	Issue ID
planning data that will not come into effect until later. Cause: The function `BAPI_EMPLOYEE_GETDATA` 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.	
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. - OR - • Disable the cache in the file `VI.Projector.SharePoint.<Version>.Host.exe.config`.	31017
If a SharePoint site collection only has read access, the server farm account cannot read the schema properties `Owner`, `SecondaryContact` and `UserCodeEnabled`. Workaround: The properties `UID_SPSUserOwner` and `UID_SPSUserOwnerSecondary` are given empty values in the One Identity Manager database. This way, no load error is written to the synchronization log.	31904
If date fields in an SAP R/3 environment contain values that are not in a valid date or time formats, the SAP connector cannot read these values because type conversion fails. Solution: Clean up the data. Workaround: Type conversion can be disabled. For this, SAP .Net Connector	32149

Known Issue	Issue ID

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>`	

There are no error messages in the file that is generated in the `PowershellComponentNet4` process component, in `OutputFile` parameter. Cause: No messages are collected in the file (parameter `OutputFile`). The file serves as an export file for objects returned in the pipeline. Solution: Messages in the script can be outputted using the *> operator to a file specified in the script. Example: `Write-Warning "I am a message" *> "messages.txt"` Furthermore, messages that are generated using `Write-Warning` are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an `Exception`. This message then appears in the One Identity Manager Service's log file.	32945
The 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	33104

Known Issue	Issue ID
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*.	
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
An error can occur during synchronization of SharePoint websites under SharePoint 2010. The method `SPWeb.FirstUniqueRoleDefinitionWeb()` triggers an `ArgumentException`. For more information, see https://support.microsoft.com/en-us/kb/2863929.	24626
Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting **File and Printer sharing** is not set on the server. This option is not set on domain controllers on the grounds of security.	24784
An error, TNS-12516, TNS-12519 or ORA-12520, sporadically occurs when connecting with an Oracle Database. Reconnecting normally solves this. Possible cause: The number of processes started has reached the limit configured on the server.	27830
Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages. Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.	29051
Valid CSS code causes an error under Mono if duplicate keys are used. For more information, see https://github.com/mono/mono/issues/7455.	762534, 762548, 29607
Memberships in Active Directory groups of type **Universal** in a subdomain are not removed from the target system if one of the following Windows updates is installed: • Windows Server 2016: KB4462928 • Windows Server 2012 R2: KB4462926, KB4462921 • Windows Server 2008 R2: KB4462926 We do not know whether other Windows updates also cause this error. The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory groups during provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem.	30575
In certain circumstances, the wrong language is used in the Stimulsoft controls in the Report Editor.	31155
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,	31998

Known Issue	Issue ID
if the `boolean` data type is redefined), it can lead to various problems in One Identity Manager.	

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 up to version 8.2.1.

Configuration Module

- New tables `QBMAdaptiveCard` and `QBMAdaptiveCardTemplate` for Starling Cloud Assistant integration.

Target System Synchronization Module

- New table `DPRProjectionObjectState` for mapping object references for synchronization.
- New column `DPRJournal.CompletionTime` for mapping the time at which synchronization ends.
- New column `DPRSystemMappingRule.ConcurrenceBehavior` for mapping the behavior of concurrent data changes.

- New column `DPRSystemMappingRule.DisableMergeModeSupport` for disabling merge mode. (

Target System Base Module

- New tables for determining a change date for groups and their memberships.
  - TSBVUNSGroupRevision
  - TSBVUNSGroupBRevision
  - TSBVUNSGroupB1Revision
  - TSBVUNSGroupB2Revision
  - TSBVUNSGroupB3Revision
  - TSBVUNSAccountBRevision

Azure Active Directory Module

- New column `AADGroup.HasReadOnlyMemberships` to map dynamic memberships.

Exchange Online Module

- New columns `O3EMailUser-RecipientTypeDetails` and `O3EMailUser.RecipientType` to improve mapping of an mail user's recipient type.

Identity Management Base Module

- New columns `QERWorkingStep.ApproveReasonType` and `QERWorkingStep.DenyReasonType` for mapping the reason type.

Changes to system connectors

The following provides an overview of the modified synchronization templates and an overview of all patches supplied from One Identity Manager version 8.2 to version 8.2.1. 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 29.

Table 14: Overview of synchronization templates and patches

Module	Synchronization template	Type of modification
Azure Active Directory Module	Azure Active Directory synchronization	changed
Active Directory Module	Active Directory synchronization	none
Active Roles Module	Synchronize Active Directory domain via Active Roles	none
Cloud Systems Management Module	Universal Cloud Interface synchronization	none
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	changed
	Oracle E-Business Suite CRM data	changed
	Oracle E-Business Suite HR data	changed
	Oracle E-Business Suite OIM data	changed
Microsoft Exchange Module	Microsoft Exchange 2013_2016 synchronization (v2)	changed
	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (v2)	changed
Google Workspace Module	Google Workspace synchronization	changed
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	None
Exchange Online Module	Exchange Online synchronization (v2)	changed
Privileged Account Governance Module	One Identity Safeguard synchronization	changed

Module	Synchronization template	Type of modification
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	changed
SharePoint Online Module	SharePoint Online synchronization	changed
Universal Cloud Interface Module	SCIM Connect via One Identity Starling Connect	none
	SCIM synchronization	none
Unix Based Target Systems Module	Unix Account Management	changed
	AIX Account Management	changed
Target System Synchronization Module	Automatic One Identity Manager synchronization	None

Patches for synchronization projects

The following is a list of all patches provided for synchronization projects in One Identity Manager 8.2.1. 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.

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

Table 15: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#34896	Improved mapping of user accounts in federations	Changes the `User` mapping to support the addition of Azure Active Directory user accounts that are later synchronized with the associated Active Directory user account. User accounts enabled for synchronization	34896

Patch ID	Patch	Description	Issue ID
		with the local Active Directory (`OnPremisesSyncEnabled = True`) only have specific schema properties read in. This patch is applied automatically when One Identity Manager is updated.	

Table 16: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#34775	Adds a password variable	Adds a variable for the synchronization user's password and replaces the password in the login credentials with the variable. This patch is applied automatically when One Identity Manager is updated.	34775

Table 17: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#21073_2	Manages mailbox permissions	Only permits principals that are also available in the Exchange Admin Center. Depends on the **Support for mailbox permissions Send as and Full access** patch. This patch is applied automatically when One Identity Manager is updated.	21073
VPR#35343_EX0	Changes the behavior of "unlimited" values	Change to the behavior of "unlimited" values. They are represented in the database as -1 instead of 0, whereby true 0 values can be handled. This patch is applied automatically when One Identity Manager is updated.	35343

Table 18: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#34938	New property mapping rule for mail user recipient type	Adds two property mapping rules for the recipient type in the `MailUser` mapping. This patch is applied automatically when One Identity Manager is updated.	34938

Patch ID	Patch	Description	Issue ID
VPR#35373	Corrects incorrect processing methods in synchronization workflows.	Removes incorrect processing methods from the **Calendar Processing** and **Mailbox Statistics** synchronization steps in the workflows. This patch is applied automatically when One Identity Manager is updated.	35373
VPR#35343_O3E	Changes the behavior of "unlimited" values	Change to the behavior of "unlimited" values. They are represented in the database as -1 instead of 0, whereby true 0 values can be handled.	35343

Table 19: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#35118	New property mapping rule for mapping ALE model names and ALE names	Adds property mapping rules for loading ALE model names and ALE names from the central system of a CUA to the `ALEModel` mapping.	35118
VPR#35370	Corrects the reference scope	Corrects the reference scope of the One Identity Manager connection to correctly map deputies to SAP user accounts. Prerequisite for the **Corrects the reference scope (for CUA)** patch. This patch is applied automatically when One Identity Manager is updated.	35370
VPR#35370_CUA	Corrects the reference scope (for CUA)	Corrects the reference scope of the One Identity Manager connection to correctly map deputies to SAP user accounts in the CUA. Depends on the **Corrects the reference scope** patch. This patch is applied automatically when One Identity Manager is updated.	35370

Table 20: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#35174_1	Allows updating of `SAPUserInSAPHRP` during provisioning (part 1/2)	Corrects the provisioning workflow to allow updating of structural profile assignments to user accounts. Prerequisite for the **Updating structural profiles during provisioning (part 2/2)** patch. This patch is applied automatically when One Identity Manager is updated.	35174
VPR#35174_2	Allows updating of `SAPUserInSAPHRP` during provisioning (part 2/2)	Corrects the synchronization configuration to allow updating of structural profile assignments to user accounts. Dependent on the **Updating structural profiles during provisioning (part 1/2)** patch. This patch is applied automatically when One Identity Manager is updated.	35174

Patches in One Identity Manager version 8.2

Table 21: General patches

Patch ID	Patch	Description	Issue ID
	Milestone 8.2.1	Milestone for the context **DPR**.	
	Milestone 8.2.1	Milestone for the context **One Identity Manager**.	

Table 22: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#28669	Support for invitations from guest users	Extends the `user` mapping for creating guest users by sending invitations.	28669
VPR#31389	Support for schema properties for hybrid environments, age groups, and user profiles	Adds new property mapping rules to the `User` mapping to support hybrid environments, age groups, and user profiles.	31389

Patch ID	Patch	Description	Issue ID
VPR#32384	Support for Azure Active Directory group license assignments	Extends the synchronization configuration to support license assignments through Azure Active Directory groups.	32384
VPR#32454	Sets the **AzureAD** tag on synchronization projects	Sets the **AzureAD** tag on synchronization projects for Azure Active Directory.	32454
VPR#32665	Synchronizes `ExternalUserState` and `ExternalUserState ChangeDateTime`	Adds property mapping rules for the schema properties `ExternalUserState` and `ExternalUserStateChange DateTime` in the `User` mapping.	32665
VPR#32975	Adds a property mapping rule for `LastPasswordChangeDate Time`	Inserts a property mapping rule for `LastPasswordChangeDateTime` into the `User` mapping.	32975
VPR#33088	Support for Azure Active Directory Service principals	Extends the synchronization configuration to support Azure Active Directory service principals and app roles. Requirement for patch **Active Directory policy support**.	33088
VPR#33198	Active Directory policy support	Extends the synchronization configuration to support Active Directory policies. Depending on patch **Azure Active Directory service principal support**.	33198
VPR#34150	Support for Microsoft Cloud US Government deployments (L4)	Adds support for Microsoft Cloud for US Government (L4).	34150
	Milestone 8.2.1	Milestone for the context **Azure Active Directory**.	

Table 23: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#32110	Adds the `middleName` schema property	Inserts the `middleName` schema property into the `User` and `inetOrgPerson` mappings.	32110

Patch ID	Patch	Description	Issue ID
VPR#32759	Adds property mapping rules for the schema property `ProtectedFromAccidentalDeletion`	Adds a property mapping rule for the schema property `ProtectedFromAccidentalDeletion` into the `user`, `contact`, `group`, and `computer` mappings.	32759
VPR#32950	Adds further property mapping rules for the schema property `mS-DS-ConsistencyGuid`	Inserts a property mapping rule for the `mS-DS-ConsistencyGuid` schema property into the `contact`, `group` and `computer` mappings. Prerequisite for patch **Corrects the property mapping rule for the schema property `mS-DS-ConsistencyGuid`.**	32950
VPR#33217_001	Checks the properties of mappings	Checks and corrects mappings that have the **Only suitable for updates** option enabled.	33217
VPR#34324	Publish group members as read only	Publish `member` properties of groups as read-only to avoid write operations in the target system browser.	34324
VPR#34715	Corrects the property mapping rule for `MSDsConsistencyGuid`	Corrects the mapping direction of the property mapping rule for the `mS-DS-ConsistencyGuid` schema property in the `user` mapping. Dependent on the patch **Adds further property mapping rules for the schema property `mS-DS-ConsistencyGuid`.**	34715
	Milestone 8.2.1	Milestone for the context **Active Directory**.	

Table 24: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#32110	New property mapping rule	Inserts a property mapping	32110

Patch ID	Patch	Description	Issue ID
	for `middleName`	rule for the `middleName` schema property into the `User` and `InetOrgPerson` mappings.	
VPR#32783	New property mapping rule for `edsvaProtectFromDeletion`	Inserts a property mapping rule for `edsvaProtectFromDeletion` in the `Group`, `Computer`, `User` and `InetOrgPerson` mappings.	32783
VPR#32952	Adds property mapping rules for `mS-DS ConsistencyGuid`	Inserts a property mapping rule for the `mS-DS-ConsistencyGuid` schema property into the `Contact`, `Group`, `Computer`, `User`, and `InetOrgPerson` mappings.	32952
VPR#34168	New property mapping rule for `edsaIsDynamicGoup`	Inserts a property mapping rule for the `edsaIsDynamicGoup` schema property into the mapping `Group`. This patch is applied automatically when One Identity Manager is updated.	34168
VPR#34634	New property mapping rules for `edsvaGFIsGroupFamily` and `edsvaCGIsControlledGroup`	Inserts property mapping rules for the `edsvaGFIsGroupFamily` and `edsvaCGIsControlledGroup` schema properties into the `group` mapping.	34634
	Milestone 8.2.1	Milestone for the context **Active Roles**.	

Table 25: Patches for Oracle E-Business Suite

Patch ID	Patch	Description	Issue ID
VPR#33804	Clearing up connection parameters	Removes unnecessary system connection parameters from the connection parameter. This patch is applied automatically when One Identity Manager is updated.	33804
	Milestone 8.2.1	Milestone for the context **Oracle E-Business Suite**.	

Table 26: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#21073	Support of the mailbox permissions **Send as** and **Full access**	Extends the synchronization configuration to support the **Send As** and **Full Access** mailbox permissions. NOTE: Since this has a large impact on performance, the corresponding synchronization steps are disabled by default and must be enabled manually.	21073
VPR#26120	New Property Mapping Rules for `IsExcludedFromProvisioning` and `IsSuspendedFromProvisioning`	Inserts property mapping rules for the `IsExcludedFromProvisioning` and `IsSuspendedFromProvisioning` schema properties into the `MailboxDatabase` mapping.	26120
VPR#27741	Supports address book policies	Extends the synchronization configuration to support address book policies for mailboxes.	27741
VPR#31470	New property mapping rule for `IsSingleItemRecoveryEnabled`	Inserts a property mapping rule for the `IsSingleItemRecoveryEnabled` schema property into the `mailbox` mapping.	31470
	Milestone 8.2.1	Milestone for the context **Microsoft Exchange**.	

Table 27: Patches for Exchange Online

Patch ID	Patch	Description	Issue ID
VPR#34170	Support for Microsoft Cloud for US Government (L4)	Adds support for Microsoft Cloud for US Government (L4). This patch is applied automatically when One Identity Manager is updated.	34170
VPR#34046	New property mapping rule for `HiddenFromExchange ClientsEnabled`	Adds a property mapping rule for the schema property `HiddenFromExchange ClientsEnabled` in the	34046

Patch ID	Patch	Description	Issue ID
		UnifiedGroup mapping.	
	Milestone 8.2.1	Milestone for the context **Exchange Online**.	

Table 28: Patches for Google Workspace

Patch ID	Patch	Description	Issue ID
VPR#32610	Mapping of different access permissions of groups	Extends the group mapping to map access permissions. This patch is applied automatically when One Identity Manager is updated.	32610
VPR#33093	Additional schema properties mapping for user accounts	Extends the user mapping to map additional schema properties of user accounts.	33093
VPR#34645	Correction in the User mapping	Corrects the property mapping rule for the Aliases schema property in the user mapping.	34645
	Milestone 8.2.1	Milestone for the context **Google Workspace**.	

Table 29: Patches for LDAP

Patch ID	Patch	Description	Issue ID
VPR#33513	Support for multiple domains with the same DN	Expands the scope and default variable set to support multiple domains with the same distinguished name.	33513
	Milestone 8.2.1	Milestone for the context **LDAP**.	

Table 30: Patches for HCL Domino

Patch ID	Patch	Description	Issue ID
VPR#25230	Changes the default value of the MailFileAccessType variable	Changes the default value of the MailFileAccessType variable to **0**.	25230
VPR#34393	Correction of a property mapping rule in person mapping	Corrects settings of the property mapping rule for InternetPassword in the person mapping. This patch is applied automatically	34393

Patch ID	Patch	Description	Issue ID
		when One Identity Manager is updated.	
	Milestone 8.2.1	Milestone for the context **HCL Domino**.	

Table 31: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#32541	Support for SSH key access requests	Adds property mapping rules to the `Asset` and `AssetAccount` mappings to support access requests for SSH keys.	32541
VPR#34392	Support of Vault for personal passwords	Inserts property mapping rules for the `AllowPersonalAccounts` schema property into the `User` mapping.	34392
VPR#34403	Handling passwords as secret values	Updates the connector scheme to treat passwords as secret values. This patch is applied automatically when One Identity Manager is updated.	34403
	Milestone 8.2.1	Milestone for the context **Privileged Account Management**.	

Table 32: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#33217_002	Checks the properties of mappings	Checks and corrects mappings that have the **Not suitable for new creation** option enabled.	33217
VPR#33301	Support of SAP S/4HANA user types and communication data	Extends the synchronization configuration to map the address and communication data of business partners.	33301
VPR#33301_2	Support for SAP S/4HANA user types	Extends the synchronization configuration to map user types.	33301
VPR#33819	New Property mapping rule for the default company of SAP clients	Inserts a property mapping rule for mapping the default company of SAP clients into the `client` mapping .	33819
VPR#34563	Correction of	Corrects the mapping and	34563

Patch ID	Patch	Description	Issue ID
	`userInRole` mapping and synchronization step	synchronization step for `SAPUserInSAPRole assignments` that are not effective. This patch is applied automatically when One Identity Manager is updated. Dependent on patch **Set filter for SAPUserInSAPRole** (VPR#31427).	
	Milestone 8.2.1	Milestone for the context **SAP R/3**.	

Table 33: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
	Milestone 8.2.1	Milestone for the context **SAP R/3 structural profile add-on**.	

Table 34: Patches for SAP R/3 BI analysis authorizations

Patch ID	Patch	Description	Issue ID
	Milestone 8.2.1	Milestone for the context **SAP R/3 analysis authorizations add-on**.	

Table 35: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
VPR#32292	Mapping of table `USOBHASH`	Inserts a map and a synchronization step to read in `USOBHASH` table data from the target system.	32292
VPR#32963_1	Mapping changes to map additional authorization objects (part 1)	Modifies various mappings to map external services, TADIR services, and RFC function modules into SAP functions. Replaces the patch VPR#32292. Part 1: Deletes existing maps. This patch is applied automatically when One Identity Manager is updated. Prerequisite for patch **Mapping changes to map additional**	32963

Patch ID	Patch	Description	Issue ID
		authorization objects (part 2).	
VPR#32963_2	Mapping changes to mapping additional authorization objects (part 2)	Modifies various mappings to map external services, TADIR services, and RFC function modules into SAP functions. Part 2: Adds new maps. This patch is applied automatically when One Identity Manager is updated. Depending on patch **Mapping changes to map additional authorization objects (part 1)**.	32963
	Milestone 8.2.1	Milestone for the context **SAP R/3**.	

Table 36: Patches for SharePoint

Patch ID	Patch	Description	Issue ID
	Milestone 8.2.1	Milestone for the context **SharePoint**.	

Table 37: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#31779	Configuration for creating and deleting site collections and sites	Expands the synchronization configuration to be able to create and delete site collections and sites.	31779
	Milestone 8.2.1	Milestone for the context **SharePoint Online**.	

Table 38: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#32564	Configuration of the number of parallel requests	Adds the variable **Max. Parallel Queries** into the default variable set.	32564
VPR#33884	Configuration of the `KeepAlive` connection parameter	Adds the **HTTP KeepAlive** variable to the default variable set.	33884
VPR#33978	New variable for setting a default	Adds a variable to the default variable set and connection parameters to be	33978

Patch ID	Patch	Description	Issue ID
	time zone	able to set a default time zone. This patch is applied automatically when One Identity Manager is updated.	
	Milestone 8.2.1	Milestone for the context **SCIM**.	

Table 39: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)

Patch ID	Patch	Description	Issue ID
	Milestone 8.2.1	Milestone for the context **Universal Cloud Interface**.	

Table 40: Patches for Unix

Patch ID	Patch	Description	Issue ID
VPR#Patch32500	**Elevation password** variable correction	Marks the **Elevation password** variable as a secret value.	32500
VPR#33249	New variables and connection parameters for authentication with the SSH private key	Inserts variables and connection parameters for authentication with the SSH private key.	33249
	Milestone 8.2.1	Milestone for the context **Unix**.	

Table 41: Patches for the One Identity Manager connector

Patch ID	Patch	Description	Issue ID
VPR#33728	Updating the One Identity Manager schema	Updates the One Identity Manager schema to support the generation of synchronization projects with the One Identity Manager connector.	33728
	Milestone 8.2.1	Milestone for the context **Database**.	

Table 42: Patches for the CSV connector

Patch ID	Patch	Description	Issue ID
	Milestone 8.2.1	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 **QER | Person | UseCentralPassword | PermanentStore** configuration parameter has been deleted.
- The **viITShop** system user has been deleted.

  Use role-based login with the appropriate application roles.
- The `VI_BuildPwdMessage` script has been deleted.

  Mail templates are used to send email notifications with login information. The mail templates are entered in the **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** and **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameters.
- The `<SpecialSheetData>` section from configuring interface forms is no longer supported. The definition now goes in the `<Properties>` section.
- The `UCI_TargetUsesProfiles` script has been deleted.

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

- The generic LDAP connector will not be supported in future. Use the new LDAP connector **LDAP Connector (version 2)**
- The SOAP Web Service will not be supported in future.
- The SPML Webservice will not be supported in future.
- The Microsoft Exchange 2010 connector will not be supported in future.
- The SharePoint 2010 connector will not be supported in future.
- The following scripts are labeled obsolete. A warning to this effect is issued during compilation.
  - VI_GetValueOfObject
  - VID_GetValueOfDialogObject
  - VI_ITDataFromOrg
  - VI_AE_ITDataFromOrg
  - VI_GetOrgUnitFromCertifier
  - TSB_CreateCanonicalNameFromDN
  - VI_ConvertDNToCanonicalName

    - VI_PersonAuto_LDAP
    - VI_PersonAuto_ADS
    - VI_PersonAuto_EBS
    - VI_PersonAuto_Notes
    - VI_PersonAuto_SAP
    - VI_PersonAuto_SharePoint_SPSUser
- Starling Two-Factor Authentication and the Starling 2FA app will no longer be supported in future versions, as the Starling Two-Factor Authentication service will be discontinued on November 1, 2022.
    - There is currently no replacement for multi-factor authentication for requests or attestation. This will be complemented by integration with OneLogin in a subsequent version.
    - Instead, use the new functionality of adaptive cards with Starling Cloud Assistant to approve request and attestation cases.

      There is still support in the Starling 2FA app in version 8.2.1 for request approvals, but it is not enabled.

      To enable the functionality for approving requests with the Starling 2FA app

        1. In the Designer, enable the `VI_ESS_PWOHelperPWO approve anywhere` process.
        2. In the Designer, disable the `QER_PWOHelperPWO approve anywhere` process.
- The **Relevance for Compliance** property for IT Shop requests (`PWODecisionStep.ComplianceRelevance` and `QERWorkingStep.ComplianceRelevance`) will no longer be supported in future versions.
- Processing of API definition code in the API Designer is being deprecated.

  Added instructions in the One Identity Manager API Development Guide on how to convert XML-based API definition code into a plugin library.
- Compilation of HTML applications in the Database Compiler is being deprecated.
- Compilation of the API DLL in the Database Compiler is being deprecated.
- The API Designer is being deprecated.
- The Visual Studio Code extension for HTML application development is being deprecated.
- Administration of different versions of a compiled project using compilation branches is being deprecated.

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 performance.
Memory	16 GB+ RAM (non-production) 64 GB+ RAM (production)
Hard drive storage	100 GB
Operating system	Windows operating system • Note the requirements from Microsoft for the SQL Server version installed. UNIX and Linux operating systems • Note the minimum requirements given by the operating system manufacturer for SQL Server databases.

Software	Following versions are supported: • SQL Server 2017 Standard Edition (64-bit) with the current cumulative update • SQL Server 2019 Standard Edition (64-bit) with the current cumulative update NOTE: The cumulative update 2 for SQL Server 2019 is not supported. NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems. • Compatibility level for databases: SQL Server 2017 (140) • 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 4.7.2 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 4.7.2 or later NOTE: Take the target system manufacturer's recommendations for connecting the target system into account. Linux operating system • Mono 5.14 or later

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

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

Minimum requirements for the application server

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 system • Microsoft .NET Framework Version 4.7.2 or later • Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and Role Services:

- Web Server > Common HTTP Features > Static Content
- Web Server > Common HTTP Features > Default Document
- Web Server > Application Development > ASP.NET
- Web Server > Application Development > .NET Extensibility
- Web Server > Application Development > ISAPI Extensions
- Web Server > Application Development > ISAPI Filters
- Web Server > Security > Basic Authentication
- Web Server > Security > Windows Authentication
- Web Server > Performance > Static Content Compression
- Web Server > Performance > Dynamic Content Compression

Linux operating system

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

Supported data systems

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

Table 43: 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):

Connector	Supported data systems
	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 2010 Service Pack 3 or later • Microsoft Exchange 2013 with cumulative update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange hybrid environments
SharePoint connector	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019
SAP R/3 connector	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.54, and 7.69 • SAP ECC 5.0 and 6.0 • SAP S/4HANA On-Premise Edition (also with SAP BASIS 7.53)
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	• SQL Server

Connector	Supported data systems
database connector	• 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, and 7.5
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 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

Connector	Supported data systems
Google Workspace connector	• Google Workspace
Oracle E-Business Suite connector	• Oracle E-Business Suite System versions 12.1 and 12.2
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard version 6.0, 6.7, 6.10, and 6.11

Product licensing

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

Upgrade and installation instructions

To install One Identity Manager 8.2.1 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 52.

Advice for updating One Identity Manager

- 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 8.2.1. 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 8.2.1, 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 or a new One Identity Manager History Database with version 8.2.1 or while updating an One Identity

Manager database or One Identity Manager History Database from version 8.0.x to version 8.2.1, 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 8.2.1, 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 8.2.1

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

To update an existing One Identity Manager installation to version 8.2.1

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.
    - To update a One Identity Manager History Database, switch to the **Other Products tab and select the One Identity Manager History Database** 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 **140** 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 8.2.1, 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.
      - To update a One Identity Manager History Database, switch to the **Other Products tab and select the One Identity Manager History Database** 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 8.2.1

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 the database server and on all the synchronization servers.

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

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

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

To update an application server to version 8.2.1

- 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 8.2.1

NOTE: Before you update the Web Designer Web Portal:

- Ensure that the application server is up-to-date.
- Ensure that the Microsoft Edge WebView2 is installed on the web server.

- 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 and install the Web Designer Web Portal again. For more instructions, see the *One Identity Manager Installation Guide*.

To update an API Server to version 8.2.1

- 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 8.2.1

- (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 8.2.1

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. 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 functions 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. 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 27
- Patches for synchronization projects on page 29

Verifying successful installation

To determine if this version is installed

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

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

  The version number 2021.0011.0019.0100 for all modules and the application version 8.2 v82-157600 indicate that this version is installed.

Additional resources

Additional information is available from the following:

- One Identity Manager Support
- One Identity Manager Online documentation

- One Identity Manager Community
- One Identity Manager Training portal website

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

Legend

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

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