One Identity Manager 8.2

Release Notes

26 November 2021, 11:54

These release notes provide information about the One Identity Manager release, version 8.2. You will find all the modifications since One Identity Manager version 8.1.5 listed here.

One Identity Manager 8.2 is a minor release with new functionality and improved behavior. See New features on page 2 and Enhancements on page 14.

If you are updating a One Identity Manager version older than One Identity Manager 8.1.x, 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

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:

General

- We are introducing inclusive terminology to our products and documentation, replacing non-inclusive terminology during the process. Changes to our user interface elements and error messages will be reflected in the documentation for each product version.
- SQL Server 2019 support with the database compatibility level **SQL Server 2017 (140)**.
- Windows Server 2022 support for Job servers, application servers, and web servers.
- Windows 11 support for workstations.
- New formatting type to prevent XSS characters being entered. The new **QBM | XssCheck** und **QBM | XssCheck | Sync** configuration parameter determines whether a check is carried out.

- Improved protection against damaging SQL statements. New configuration parameters for risk assessment, **QBM | SQLCheck | RiskEvaluation** and **QBM | SQLCheck | SubSelect**.
- Support for a connection pool for separate sessions for reading and writing on different database servers. In the connection dialog, the **Data Source** property can contain a pipe (|) delimited list of servers. The first server specified is the primary server used for write access. All other servers are read-only copies with read access only.
- For password policies, you can specify how many character class rules must be satisfied for a password to match the password policy.
- Advanced configuration for OAuth 2.0/OpenID Connect.
  - The OAuth 2.0/OpenID Connect configuration for identity providers can be taken from a template. For the One Identity Redistributable STS (RSTS), the file is pre-configured. You can find the `RSTS_Template.xml` in the One Identity Manager installation directory. The template can be used in the Designer.
  - You can specify whether a check of the ID token takes place.
  - You can specify the acr values that the authorization server can use for processing an authentication request.
  - You can specify the claim type to be additionally checked.
  - You can configure the behavior of the client after logging off from the application.
- Support for authentication of external applications via OAuth 2.0/OpenID Connect.

  There are new **QBM | AppServer | AccessTokenAuth** and **QBM | AppServer | AccessTokenAuth | RoleBased** configuration parameters provided for configuration.
- Fallback for login using OAuth 2.0/OpenID Connect authentication modules for determining users. If no matching person is found for the claim value, the authentication modules search for the claim value in the system users' permitted logins (`DialogUser.AuthentifierLogons`). If an entry is found there, then that system user is logged in.
- Individuals who are considered a security threat will no longer be able to log in to One Identity Manager. To allow login, set the **QER | Person | AllowLoginWithSecurityIncident** configuration parameter.
- A new table `QBMColumnLimitedValue` has been implemented to map lists of permitted values. A new table `QBMColumnBitMaskConfig` has been implemented to map bit masks. Editing is done in the Designer's Schema Editor on the **Value properties** tab. Default values can be deactivated on a custom basis.
- You can specify whether to check if single MVP column values have to be unique, case sensitive, or accented characters. Editing is done in the Designer's Schema Editor on the **Value properties** tab.
- For unique groups of columns, you can enter message texts to be used instead of the default error message.

- The query type of predefined database queries can be used to specify whether an entire SQL query is being handled or just the Where clause section.
- If the format is specified, the target type of the expression is a `string`. If the format is not specified, it is the specified data type.
- You can specify whether a Job server participates in load balancing.
- In custom method definitions, a script can be used to conditionally display a method. For example, this way you can control whether a task is only displayed in the Manager if a certain condition is met. The script does not change the user's permissions, only the behavior when loading an object in the One Identity Manager tools.
- New features for schedules.
  - Schedules can be run on a specific day of the week in a specific month.
  - Multiple start times can be set per day.
  - The start details of schedules is logged.
- You can define a default country that is taken into account when determining working hours and holidays.
- Extension of $ notation with optional format specification: `$<definition>:<data type>{<format>}$`
- Introduction of a new One Identity Manager query language. The One Identity Manager query language can be used to create queries or Where clause expressions against the One Identity Manager object layer.One Identity Manager For example, the One Identity Manager query language is used to communicate between application servers and clients. Currently, you can use the One Identity Manager query language in the Object Browser's query window . For more information, see the *One Identity Manager Configuration Guide*.
- Support for custom configuration files for logging with NLog. The `custom-log-variables.config` and `custom-log-targets.config` include files are defined in the `globallog.config` file. The `LogFileLevel` variable can overwrite the severity level in a custom configuration file. The `eventLogLevel` variable can be used to override the information level in a custom configuration file.
- Transport templates can be created with the Database Transporter. You can use the transport templates when you create transport packages with the Database Transporter or with the `DBTransporterCMD.exe` command line program. This loads the export criteria from the transport template file.
- The `DBTransporterCMD.exe` command line program supports the transport of synchronization projects.
- New feature in the `Quantum.MigratorCmd.exe` command line utility.
  - Support for creating, checking, and extending SQL Server logins if granulated permissions are used.
  - New mode for creating an operational database after the database has been restored from a backup.

- The `DBCompilerCMD.exe` command line program supports automatic compilation of the database. The database is monitored and compiled if necessary.
- The `AutoUpdate.exe` command line program supports automatic software updating of a One Identity Manager installation.
- The One Identity Manager tools are displayed in the Launchpad in a new **Programs** menu item and can be started from there.
- Individual tasks in the Launchpad are also available for users with role-based permission groups.
- An email configuration wizard is provided to configure email functionality in the One Identity Manager. The wizard can be run in the Launchpad and in the Designer's Configuration Parameter Editor.
- The user interface of some One Identity Manager components requires Microsoft Edge WebView2 to display certain content. When installing the components, Microsoft Edge WebView2 is also installed.
- The application server can be limited to a REST API mode.
- Automatic updating of the application server can be configured in the `web.config` file. The `mode` attribute can be used to control whether the update is scheduled or started manually.
- New **Common | Indexing | DefaultResultLimit** configuration parameter to specify the maximum number of search results returned for a query.
- The API Server optionally provides a SCIM V2.0 interface through a plugin. This allows read and write access to a defined set of One Identity Manager tables.
- The availability of a One Identity Manager Service can be tested over /alive.
- New `DirectConnection` setting to configure the One Identity Manager Service for directly connecting to the target database without availability testing.
- New `DoNotWriteConfigBack` setting to configure the One Identity Manager Service not to write the configuration back to the database.
- New FtpComponent process component. This process component can transfer files by SFTP.
- New `CallMethodExclusive` process task for the process component `HandleObjectComponent` to exclusively call a customizer method.
- The F1 help and One Identity Manager documentation are provided in HTML5 format. You can access One Identity Manager documentation in the Manager by selecting the **Help > Search in local help** menu item.
- Integration of Customizer methods into the Typed wrapper classes.
- Step-by-step preparation of a database update. This runs through the various phases for preparing the database update. This step-by-step preparation is intended to ensure that users are informed about the upcoming update and that processes can be shut down in a targeted manner.

  > NOTE: Step-by-step preparation is used only when updating databases that have at least One Identity Manager version 8.2.

Web Portal

- This One Identity Manager version includes fundamentally redesigned web applications based on HTML5 technology. These web applications are provided through the API Server and cover the following application areas, among others:
  - IT Shop requests and approvals
  - IT shop configuration
  - Management of identities, user accounts, system entitlements, company structures, and system roles
  - Application Governance
  - Management of attestation policies
  - Attestation case approvals
  - Password management
  - Job queue process monitoring

  > NOTE: The web applications that were previously part of the product are still available. For reasons of understanding, a distinction is now made between the Web Designer Web Portal and the Web Portal.

- Application Governance is now part of the Web Portal. Application governance functionality lets you quickly and easily centralize the onboarding process for new applications. A new application combines all the entitlements that application users need for their daily tasks. This allows you to assign application permissions (for example, system entitlements or system roles) to your application and plan when they will be available in the Web Portal as requestable products.
- In the Operations Support Web Portal it is now possible to view objects marked as outstanding, delete these objects in the database, or add them back to the target system. Additionally, it is possible to reset the status of these objects so that they are no longer marked as outstanding. A new **Basic Roles | Operational Support | Post Synchronization Handling** application role is provided.
- It is now possible to decide in the Operations Support Web Portal how to deal with failed processes. For example, you can re-run processes and process steps that contain errors.
- It is now possible to assign new passwords to identities in the Operations Support Web Portal.
- In the Web Portal, you can display and request products that other people from your vicinity have already requested. As a manager, you can also see products from your team’s peer groups.
- It is now possible to create, edit, and delete sample data in the Web Portal. This sample data can then be used in attestation policies to perform attestations for only a subset of objects, for example, if attesting all objects would take too long.
- In Web Portal you can now display an organizational chart for each identity.
- In the Web Portal, there is now a **Products expiring soon** tile on the home page that indicates products that will expire in the near future and need to be renewed.

- Memberships in objects that were created through dynamic roles can now be excluded in the Web Portal.
- It is now possible to create, edit, and delete shops and associated shelves in the Web Portal.
- Using the Administration Portal, you can now view and edit your API configuration.
- It is now possible to provide your own HTML5 applications as a ZIP file and have them hosted over the API Server.
- It is now possible to create, edit, and delete service categories in the Web Portal.

Target system connection

- Support for Microsoft Teams.

  Microsoft Teams teams and channels are mapped in One Identity Manager. The Microsoft Teams connector has the task of synchronizing Azure Active Directory. Installing the Microsoft Teams Module provide synchronization templates for Microsoft Teams. The Azure Active Directory connector uses the Microsoft Graph API for accessing Microsoft Teams. For more information, see the *One Identity Manager Administration Guide for Connecting to Microsoft Teams-Umgebung*.

  A patch for synchronization projects with patch ID VPR#32454 is provided.
- Simulation of property mapping for single objects

  In the Synchronization Editor, you can test the results of property mapping rules. In particular, this can be used to check the mapping of virtual schema properties. The test results can be exported and thus used for product support.
- Support for the Microsoft Cloud for US Government (L4) national cloud deployment.

  Patches for synchronization projects with patch ID VPR#34150 and patch ID VPR#34170 are provided.
- Support for Azure Active Directory guest users. To send the invitation to guest users, additional modifications are required in the synchronization project.

  Patches for synchronization projects with patch ID VPR#28669 and with patch ID VPR#32665 are provided.
- For Azure Active Directory user accounts, additional properties are supported for mapping personal and federation information for Azure Active Directory.

  A patch for synchronization projects with patch ID VPR#31389 is provided.
- The date of the last password change to Azure Active Directory user accounts is loaded.

  A patch for synchronization projects with patch ID VPR#32975 is provided.
- Support for license assignment to Azure Active Directory user accounts through Azure Active Directory groups. Additional reports are provided for user accounts and subscriptions.

  A patch for synchronization projects with patch ID VPR#32384 is provided.
- Support for Azure Active Directory applications, service principals, and app roles.

A patch for synchronization projects with patch ID VPR#33088 is provided.

- Support for Azure Active Directory activity-based timeout policies, home realm discovery policies, token issuance policies, and Token lifetime policies.

  A patch for synchronization projects with patch ID VPR#33198 is provided.

- Update employees when Azure Active Directory user accounts are changed.

  The new **TargetSystem | AAD | PersonUpdate** configuration parameter can be used to control whether the properties of connected employees in One Identity Manager are updated when user accounts in Azure Active Directory are changed.

- Support for custom Azure Active Directory schema extensions. The Azure Active Directory connector can read and write Azure Active Directory schema extensions.
- The Azure Active Directory connector supports delta synchronization to speed up Azure Active Directory synchronization. Delta synchronization is not enabled by default, it must be customized.
- The **Hide group from Outlook** property in Office 365 groups is mapped.

  A patch for synchronization projects with patch ID VPR#34046 is provided.

- The Active Directory connector supports Active Directory, which is shipped with Windows Server 2022.
- With Active Directory synchronization, more restrictive values for the minimum password length and the number of passwords to store are applied from a domain's global account policy to the One Identity Manager password policy for that domain.
- The **Middle Name** property of Active Directory user accounts is mapped.

  A patch for synchronization projects with patch ID VPR#32110 is provided.

- Support for protection against accidental deletion of Active Directory containers, user accounts, contacts, and computers.

  Patches for synchronization projects with patch ID VPR#32759 and with patch ID VPR#32783 are provided.

- The Azure AD Connect anchor ID of Active Directory user accounts, contacts, groups, and computers is mapped.

  Patches for synchronization projects with patch ID VPR#32950 and with patch ID VPR#32952 are provided.

- The Password Capture Agent supports Windows Server 2019 and Windows Server 2022.
- Support for One Identity Active Roles version 7.4.5.
- Support for the Active Roles Group Family.

  A patch for synchronization projects with patch ID VPR#34634 is provided.

- A new **TargetSystem | ADS | ARS** configuration parameter has been added Active Roles. Active Roles specific components are marked with a new preprocessor condition **ARS**.
- Support for the Microsoft Exchange mailbox permissions **Send as** and **Full access**.

A patch for synchronization projects with patch ID VPR#21073 is provided. Synchronization is not enabled by default. In request to synchronize mailbox permissions, the synchronization project must be customized.

- Support for excluding Microsoft Exchange mailbox databases from automatic mailbox distribution.

  A patch for synchronization projects with patch ID VPR#26120 is provided.

- Support for Microsoft Exchange address book policies.

  A patch for synchronization projects with patch ID VPR#27741 is provided.

- Support for recovery of individual items of Microsoft Exchange mailboxes.

  A patch for synchronization projects with patch ID VPR#31470 is provided.

- A new LDAP connector **LDAP connector (version 2)** is provided. Project templates are provided for OpenDJ, Active Directory Lightweight Directory Services (AD LDS), and Oracle Directory Server Enterprise Edition (DSEE), as well as a generic project template.
- Support for multiple linking of LDAP systems with the same distinguished name.
  - With newly created synchronization projects, the LDAP domain names are formed with `<DN component 1> (<server from connection parameters>)`.
  - For existing synchronization projects created with the generic LDAP connector, a patch with patch ID VPR#33513 is provided.
  - LDAP domains that are already in the database are not renamed. If necessary, manually adjust the LDAP domain names (`Ident_Domain`).
- Support for the One Identity Safeguard versions 6.7, 6.10, and 6.11.
- Support for access requests for SSH keys for One Identity Safeguard.

  A patch for synchronization projects with patch ID VPR#32541 is provided.

- Support for vault for personal passwords for user accounts in One Identity Safeguard.

  A patch for synchronization projects with patch ID VPR#34392 is provided.

- Connection of PostgreSQL databases

  With the generic database connector, PostgreSQL databases can now also be connected.

- The One Identity Manager connector supports synchronization of databases with different product versions or different number of modules.

  A patch for synchronization projects with patch ID VPR#33728 is provided.

- Generation of synchronization projects for synchronization of two One Identity Manager databases (system synchronization)

  The synchronization project for synchronization of two One Identity Manager databases can be created automatically based on defined criteria. This creates an image of selected application data from a One Identity Manager database. Support for revision filtering. The frequency of synchronization can be set individually for each table to be synchronized.

System synchronization simplifies the setup and maintenance of the synchronization configuration. One Identity Manager takes care of setting up all the components of the synchronization configuration. Manual adjustments are not necessary. For example, use system synchronization to outsource computationally intensive functions such as attestation and automatic revoking entitlements from the central database.

A patch for synchronization projects with patch ID VPR#33728 is provided.

- The scope of the synchronization protocol has been extended. Information about the processed objects, synchronization progress, revision filtering by synchronization step is now output. The level of detail can be configured in the synchronization workflows.
- Variables can be used for defining quotas.
- The Oracle E-Business Suite connector and the generic database connector for Oracle Database have been migrated to Oracle Data Provider for .NET (ODP.NET).

  A patch for synchronization projects with patch ID VPR#33804 is provided.

  > IMPORTANT:
  >
  > - The connection parameters of existing synchronization projects for Oracle E-Business Suite are altered when establishing the connection to the target system, where possible, and should be checked afterwards.
  > - The connection parameters of existing synchronization projects for the generic database connector for Oracle Database are altered when updating One Identity Manager, where possible, and should be checked afterwards.

- Mapping of different types of system entitlements

  Many cloud applications use more than one group type to map entitlements. When connecting cloud applications, other types of system entitlements, such as roles or entitlement sets, can now be mapped in addition to groups. Depending on the target system, assignments are maintained either with the user accounts (user-based assignment) or with the system entitlements (entitlement-based assignment). The types used and with which object types the assignments are maintained is configured when synchronization is set up.

  The different types of system entitlements and their assignments can be integrated into Identity Audit and attestation.

- When defining schema types in a schema extension file for the SAP connector schema, the `InsertCommitDefinition`, `WriteCommitDefinition`, and `DeleteCommitDefinition` attributes can now also be used.
- SAP S/4HANA user types and communication data are supported.

  Patches for synchronization projects with patch ID VPR#33301 and VPR#33301_2 are provided.

- An RFC function module `/VIAENET/HELPER` with the `/VIAENET/ZHELPER` function group is provided, which selects the `PA0002` table.

- An RFC function module /VIAENET/READTABLE is provided, which behaves similarly to the RFC_READ_TABLE function module. The function can read data from tables and views in the SAP database, as long as they are not marked as internal tables.
- For mapping additional HR data to employees, the **SAP R/3 HCM employee objects** synchronization template provides the mapping and the Employee_PA0000 synchronization step. This mapping can be used instead of the default Employee mapping. To do this, activate the Employee_PA0000 synchronization step and deactivate the Employee synchronization step.
- The Domino connector supports the Notes Client version 10.0.
- Support for HCL Domino Server version 12.0 and HCL Notes Client version 12.0

  > NOTE: If the connected Domino system uses Domino 12 and the Domino connector has write access to the target system, then the gateway server must have Notes client version 12 installed.
  >
  > If read-only access to the target system is required, an older Notes client version can also be used on the gateway server.

- Creating SharePoint Online site collections and sites

  You can add new site collections and site in the One Identity Manager and publish them in the SharePoint Online target system. Predefined scripts and processes are provided for this purpose. These can be used as templates to make site collections and sites requestable through the IT Shop.

  A patch for synchronization projects with patch ID VPR#31779 is provided.

- For synchronization of Unix-based target systems, authentication with a private SSH key is supported.

  A patch for synchronization projects with patch ID VPR#33249 is provided.

Identity and Access Governance

- Improved support for inheritance of target system-specific groups and permissions by user accounts.

  To better distinguish which types of groups and permissions are inherited, additional options for inheritance have been implemented. In addition, you can specify which groups and privileges are to be inherited when you create the account definitions. A note is displayed on the user account overview forms when groups and permissions cannot be inherited.

- For inheritance of groups and permissions based on categories, 64 categories can now be created.
- Assignments of employees to multiple business roles can be prevented. You can enable the option for role classes and role types.
- New default approval procedures **KA** and **OT** for attestations and IT Shop requests.
- New default approval procedure **CS** for attesting employees.
- New default objects (attestation policy, attestation procedure, condition types, approval workflow, and approval policy) for attestation of initial manager

assignment. With this attestation, missing manager information can be requested and assigned to employees.

- New report **Overview of the results of an attestation run**.
- Attestation policies can be configured to automatically change the certification status of attestation objects when an attestation is approved or denied. The **Set certification status to "Certified"** and **Set certification status to "Denied"** options can be enabled if a table is selected in the attestation procedure that has an `ApprovalState` column. The feature can be used by default for attesting employees, business roles, application roles, and organizations.
- Shortened process of attestations if an attestor is authorized to make multiple approvals in one attestation case. If this attestor grants approval it is automatically carried over to subsequent approval steps. Thus, the attestation case is submitted to the attestor for approval only once.

  The feature is activated with the **QER | Attestation | ReuseDecision** configuration parameters.
- Sample attestation

  With sample attestation, attestation cases can be restricted to a selection of attestation objects. Samples can be compiled manually or based on defined criteria. A default sample **Monthly organizational changes to employees** is provided. This can be used if the **QER | Selections | PersonOrganizationalChanges** configuration parameter is set. To create random samples, the `QER_PPickedItemInsertRandom` SQL procedure can be used.
- Weekends and public holidays are now taken into account by default when calculating working hours, for example for the due date of attestation cases or the approver reminders. To configure whether weekends or holidays should be treated as working days, additional configuration parameters have been introduced.
  - QBM | WorkingHours | IgnoreHoliday
  - QBM | WorkingHours | IgnoreWeekend
  - For time-limited requests, if the expiration date has passed, requests can now go through a cancellation workflow before the assignment is permanently removed.
  - QER | Attestation | UseWorkingHoursDefinition
- Assignments of company resources to system roles can now be requested in the Web Portal. For this purpose, the **Assignments to system roles** default assignment resource is provided.

  When attesting assignments to system roles, the requested assignments can also be removed automatically. The **QER | Attestation | AutoRemovalScope | ESetHasEntitlement | RemoveRequested** configuration parameter was introduced for this purpose.
- The definition of SAP functions has been extended so that external services, TADIR services and RFC function modules can be included in the authorization check in addition to transactions. Transactions, external services, TADIR services, and RFC

function modules are mapped as SAP applications in One Identity Manager.

Patches for synchronization projects with patch ID VPR#32963_1 and VPR#32963_2 are provided.

- The definition of product-specific request properties has been redesigned. Now you can define a lot of additional information for request parameters. This makes the implementation of request properties more flexible. The previous solution can still be used. When creating new request properties, you specify whether you want to use the modern or the obsolete definition.
- Assigned requests that have passed their expiration date can now go through the cancellation workflow stored in the approval policy before the assignment is finally removed. The feature is activated with the **QER | ITShop | ExceededValidUntilUnsubscribe** configuration parameters.
- Employees can excluded automatically from dynamic roles on he basis of a denied attestation or a rule violation. An excluded list is maintained to do this. Excluded lists can also be defined for individual employees.
- Support for the reorganization of a IT Shop solution. The following tasks can be run on custom IT Shop structures:
    - Simultaneous moving of several selected products from one shelf to another shelf.
    - Moving a complete shelf to another shop.
    - Moving a complete shop to another shopping center.
- Introduction of a general deputization of all an employee's approval entitlements. An employee can appoint a deputy for all approval powers in one area. This deputy is additionally identified as the approver for all approvals that the employee is required to make during a specified time period. Deputies may be established for attestation, request approvals, and exception approvals of requests.
- When attesting memberships in application roles, memberships that were created through a dynamic role can also be automatically removed. The **QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDynamicRole** configuration parameter was introduced for this purpose.
- Google Workspace admin role assignments can now be requested in the Web Portal and integrated into Identity Audit.
- Manually created application roles for product owners are now also automatically deleted if they are not used.

    > NOTE: If you have set up your own application roles under the **Request & Fulfillment | IT Shop | Product owners** application role that you use for custom use cases (tables), then check whether these can be deleted automatically. Otherwise, disable the **Clean up application role "Request & Fulfillment | IT Shop | Product owners"** schedule.

See also:

- Enhancements on page 14
- Resolved issues on page 28

- Schema changes on page 42
- Patches for synchronization projects on page 62

Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.2.

Table 1: General

Enhancement	Issue ID
The overview of the system configuration has been improved and extended with new values. • The report can be saved as a CSV file • The database encryption state is displayed. • Improved display of historical data values.	31738, 32890, 32992, 34692
Improved support for the delta method for faster database updates.	32791, 32917
Improved migration performance.	34109, 34587, 34591
The **basegroup** database role is no longer used. The database role is no longer created for new installations. In existing installations the database role can still be used.	34179
Improved creation of table indexes.	33530
Improved readability of generated view definitions.	31491
New consistency check **Mandantory field definition missing** to detect potentially missing mandatory field definitions.	31297
The default language of a language code (`QBMCulture.UID_DialogCultureDefault`) can be customized.	31749
Entries are now generated in the `DialogProcess` table for deferred operations.	32782
Improved determining of process information about a trigger.	34529
Improved support for BULK operations in the object layer.	31066, 31573, 32249
Improved support for retrieving historical information.	30334, 30437, 31449,

Enhancement	Issue ID
	31450, 31451, 34723
Extension of EntityLogic fluent interfaces for running conditionally.	33796
Optimized determining display values.	33931
The hash function SHA-1 is not used anymore.	27488
Improved password quality calculation. Password quality for short passwords can now be lower.	33683
Permissions of logins for administrative users with granulated permissions are extended in the Configuration Wizard, if necessary.	30904
Existing SQL Server logins can be used in Configuration Wizard.	30791
Improved enabling and disabling of authentication modules in the Designer.	33929
The `<SpecialSheetData>` section from configuring interface forms is no longer supported. The definition now goes in the `<Properties>` section. NOTE: Existing configurations will be adjusted during the database update. Check the data if necessary.	31332
Improved documentation of supplied schedules by default.	32506
Improved documentation for overriding templates.	33215
Improved support for uninstalling One Identity Manager components. As long as there are multiple One Identity Manager installations, the configuration data cannot be removed.	31159
In the connection dialog, the database server can now be deleted from the server menu.	32510
When running multiple databases in a managed instance in Azure SQL Database, you can fix the number of slots in the new **QBM | DBServerAgent | CountSlotAgents** configuration parameter.	34047
Improved support for installing modules later.	33942
Improved documentation of the DBQueue Processor reinitialization after a server hardware upgrade.	34208
The `StdIoProcessor.exe` checks whether its parent process (`VINetworkService.exe`) is still up and running.	31081
Improved logging of process handling in the One Identity Manager Service log file.	31536, 32792, 33721, 34330,

Enhancement	Issue ID
	34559
Improved output of table names in error number 810005.	31686
New **Server\Job Server\Configuration utility** machine role for installing the Job Service Configuration.	32776
The Server Installer remembers the directory with the installation files.	33686
Improved installation information for the One Identity Manager Service in the Server Installer and in the Configuration Wizard.	34457
A time delay is now in effect when exiting the One Identity Manager Service to allow the service to synchronize with the database.	34459
Support for custom translations of resource file text.	23677
The Where Clause Wizard for entering database queries supports date comparisons.	17996
Improved feedback for the system status in the One Identity Manager tools' status bar.	29567
The status bar indicates whether the logged-in user is an administrative user.	33491
Update of the controls in the One Identity Manager tools.	31577
Improved display of multi-line values in MVP columns.	31312
Improved display of columns representing a URL.	33545
If a text is too long for translation, a corresponding hint is now displayed at the input field.	33667
To make filters available to all users, you can publish the filters in the Manager or in the Designer, for example.	31025, 33247
Improved display of the primary key in an object's properties dialog. The primary key can be copied in different formats.	32549
Improved SQL export in an object's properties dialog.	33679
Improved support for script editing. • The functions in the advanced editing window for scripts have been revised and extended. • Additional code snippets are provided. • Sorting of the code snippets has been improved.	32026, 32937, 33161, 33162, 33240
Display values for report parameters can be passed to reports.	34272
The maximum number of result rows of report queries can now be modified.	34293
Tooltips are displayed on assignment forms in the Manager.	31634

Enhancement	Issue ID
Outstanding objects are now shown crossed out on the assignment forms.	34508
In the Object Browser, breakpoints are automatically saved in the configuration when the debug dialog is closed and loaded again when the debug dialog is reopened.	30816
Improved prompt when saving changes in the Object Browser.	31291
In the Object Browser, when SQL queries are run, the total number of times and the run time of the query are output.	31813
Enhancements and improvements in the Job Queue Info. • Parameters that contain an object key are displayed as a link. The link displays the object properties. The Object Browser can be started. The Synchronization Editor can be started if the object keys refer to a synchronization project. • A new start time for a process step can be set. • The number of retries for a process step can be changed. • Multiple Job servers can be selected at the same time to edit the credentials to determine the status.	30102, 31983, 32851, 33516, 33642
In the Software Loader the root directory is now stored per database.	29507
In the Database Transporter, test whether the logged-in user has sufficient permissions to import.	34704
Improved behavior of the web service integration wizard.	31425
Improved support for mail definitions in the Designer.	31820, 33419
In the Designer, modified configuration parameters are specially flagged in the Configuration Parameter Editor.	32566
Improved support for editing table relations. Dynamic table relations are now displayed in the Schema Editor.	31849, 32582, 32429
View definitions can be checked in the Schema Editor.	33170
In the Script Editor, the font size can be changed using **Ctrl + mouse wheel**.	32026
The Process Editor points out possible misconfigurations when checking process validity.	32035, 34223
Improved column configuration support in the Schema Extension.	32436
Improved behavior of the command line tools.	30328, 31082,

Enhancement	Issue ID
- Version, error messages, and help texts are output. - In the `/conn` parameter of the command line tools, the name of the connection can be entered according to the `HKEY_CURRENT_USER\Software\One Identity\One Identity Manager\Global\Connections` registry entry.	34077, 34209, 33010
Improved detection of need to compile in the `DBTransporterCMD.exe` command line program.	32062
Improved support for importing files with the `SoftwareLoaderCMD.exe` command line utility.	33943
Documentation of the `create-web-dir.exe` command line program.	33618
When closing the Launchpad with the **Close** button, a notice is now displayed that the Launchpad is minimized to the notification area of the Windows task bar.	31984
The Launchpad shows the color of the staging layer in the status bar.	32593
The PowerShell library for One Identity Manager has been extended.	33127

Table 2: General web applications

Enhancement	Issue ID
Improved security in the application server.	32466
REST API application server enhancements and improvements .	32576, 33963, 33728, 33126, 32930, 33923, 34016
Improved session handling in the application server when using tokens to authenticate.	33406
The validity of the session certificate is checked.	32141
In the application server, it is now possible to access the API with requests authenticated by access tokens.	245784
The **VI_ITShop_Compliance_DoNotCheckIndirect** Web Designer configuration key has been removed.	33042
For security reasons, the **VI_Common_UserMessageAdd HTML** Web Designer component now encodes the entered text by default. This behavior can be deactivated by the `DoNotHtmlEncode()` virtual function when calling the component.	202604

Enhancement	Issue ID
For security reasons, the **VI_Common_ExternalFormHost** Web Designer component can now no longer be used to display arbitrary URLs. If you need this functionality, you must rebuild existing code and use the **QBM_Common_ExternalFormHost** form component instead. This has the advantage of not passing URLs in the form of URL parameters.	203559
The parameter **withPermissions** of the Web Designer function `dbcount()` is now marked as obsolete.	34222
The permissions for debugging web applications have been extended.	34308
Webauthn security keys: The RSTS version has been updated to version 2019.11.22.0. You can now prevent the X-Frame-Options HTTP response header from being output at all by setting the RSTS configuration property **DisableAddingXFrameOptionsHeader** to **true**.	206688
Identities with the **Basic roles | Operational support** application role can now no longer start and stop the DBQueue and JobQueue. If identities are to perform these tasks, they must be assigned the **Basic Roles | Operational support | System administrators** application role.	34368
Improved performance of grid controls. Less database queries are generated.	206856
When an request item is removed from a shopping cart that has dependent products, the dependent request items are also removed.	32758
When a shopping cart is deleted, its request items are also deleted.	33342
Improved presentation of the results of a peer group analysis.	34190
Managers now see all the delegations of their child identities in the Web Designer Web Portal and in the Web Portal.	33774
It is now possible to set a default size for images. When uploading images to Web Portal, they will be scaled accordingly.	32916
Shopping carts that have already been sent are now marked accordingly and it is no longer possible to add more products to such shopping carts.	33143
In the Web Portal, the request's main data now displays the request status instead of the processing status.	34181
Improved warnings have been introduced for the Web Portal log file and for the Web Portal monitor page, which indicate components that load a conspicuously large number of objects.	206672
Removed check box in front of the date field in the Web Portal. If you do not want a time restriction, do not enter anything in the field.	206732
If a single sign-on session ends in the Web Designer Web Portal, a button is now displayed that can be used to log in again with single sign-on.	206886

Enhancement	Issue ID
In the Web Portal, the set of selectable reference users is limited in the default configuration.	246899
The dialog for deleting secondary memberships of a role in the Web Portal has been extended. It now offers the possibility to optionally delete direct, requested, and dynamic memberships respectively.	250631
In the Web Portal, memberships in system entitlements can now be filtered and paginated.	275192
The label in the **Filter on** filter dialog has been changed to **Filter on the '<column name>' column**.	274174
In the Web Portal, an error message is displayed if the date entered is invalid.	33056
The following columns in the `QBMWebApplication` table have been described in such a way that it is clear that they are only relevant for the Web Designer Web Portal: • UID_DialogAEDSWebProject • UID_DialogAuthentifier • UID_DialogAuthSecondary	34334
Improved design and navigation of the Operations Support Web Portal.	278209
For performance reasons, the API Server result format has been changed so that the value of **DisplayValue** is only sent if it differs from the value of **Value**.	206530
The `imx/ping` API method has been introduced for the API Server. This API method can be used as a "health check" of the API Servers. It can be called without authentication.	206652
It is now possible to configure the logging of the API Servers using a central configuration file.	206728
The API Server now returns unset dates in the JSON serialization as **NULL**.	239140
For the API Server, the Microsoft Extensibility Framework component has been removed. NOTE: • Marking classes with the `[Export]` or `[Import]` attributes is no longer supported. • All public classes that implement a given interface are automatically found as a plugin. • Plugin classes must no longer be marked as "internal". Plugin classes must define a public and parameterless constructor.	240595

Enhancement	Issue ID
The API Server now supports HTTP compression.	265172
A content security policy has been introduced for HTML5 applications.	203857
The source code structure for HTML5 applications has been changed to an Angular workspace to enable a uniform folder structure without symbolic links.	226217
The API Server provides the HTML5 web application documentation.	268196
Halted requests no longer appear in HTML5 web application logs.	271770
For performance reasons, bulk entity processing can now be configured when configuring entity-based API methods.	228139
The entity schema must now be queried at runtime by the API Server.	251938
The following changes have been made to the API model for hierarchical entity structures: • The **DisableHierarchicalData** flag in the API definition has been removed. • The **noRecursive** URL parameter has been removed. The **ParentKey** URL parameter can be used to control whether results from the top level, a specific level, or all levels of the hierarchy should be returned.	273103

When an API method is defined, not all columns are made writable by default. When developing API methods, the columns must be declared individually or explicitly all made writable.
Example:
`Method.Define("some_url")`
`.From("Person")`
`.EnableUpdate()`
`.WithWritableColumns("FirstName", "LastName")`
	274045

The Internet Explorer is no longer supported.	273336
Update of the Secure Password Extension to version 5.9.5.	34834

Table 3: Target system connection

Enhancement	Issue ID
Customizer methods are provided to handle outstanding objects in an automated manner. These methods can be called in scripts or processes.	29566
Improved logging of synchronization errors using NLog.	30992

Enhancement	Issue ID
Improved documentation of quotas in synchronization steps.	31927
The synchronization buffer can be disabled for schema properties in the One Identity Manager schema that map members of many-to-many schema types or key resolutions. IMPORTANT: If the synchronization buffer is disabled, references that are missing in One Identity Manager will be deleted in the target system when synchronizing into the target system or during provisioning. Therefore, check carefully whether the synchronization buffer can be disabled.	31947
New consistency check **Outstanding objects with not outstanding assignments** to determine outstanding objects with assignments that are not outstanding.	32058
The Synchronization Editor can be run in offline mode when access to the connected system is not required.	32181
The One Identity Manager connector detects if the Customizer sets default values for mandatory fields.	32346
When automatically creating or updating synchronization projects using a command line command or Windows PowerShell CmdLet, a remote connection can now be used to connect to the target system.	32411
In the Synchronization Editor log view color is used to show whether a synchronization was completed successfully or with errors.	32517
When setting up a new synchronization step, a quota of **10%** is set by default for objects in One Identity Manager for the `Delete` processing method. This quota can be adjusted on a project-specific basis.	32740
The home page of the Synchronization Editor shows whether patches are available for existing synchronization projects.	32795
To restart a start up sequence if it was unexpectedly stopped, the instance of the start up sequence can be deleted directly in the Synchronization Editor.	33050
The schema view of the mapping editor now shows which schema property contains the revision counter.	33064
Copies of synchronization projects can now be created in the Synchronization Editor.	33280
Improved membership provisioning when members of an object in One Identity Manager are mapped to different member lists of an object in the target system.	33449
Schema properties with the **Property join** property type (`PropertyJoin`) are now writable.	33417

Enhancement	Issue ID
In synchronization projects with the generic database connector, the Windows PowerShell connector, and the CSV connector, a subtype can be entered for each connected system. One Identity Manager needs this information to provision memberships if the objects from several similar generic target systems are mapped in the same One Identity Manager tables.	33426
The Synchronization Editor prevents synchronization projects from being edited and saved simultaneously by multiple users.	33753
Improved revision filtering support.	34101, 34102
The behavior of start up sequences can be configured such that a start up sequence starts multiple times, although multiple start ups are not allowed. The new instance of the start up sequence can be stopped with an error (default behavior) or stopped non-verbosely.	34114
Improved error message for the error: `Automatic resolution of the failed workflow's dependencies.`	34140
The Synchronization Editor Command Line Interface can be used to update the One Identity Manager schema in synchronization projects.	34117
The condition for applying a property mapping rule can now also be formulated as a script.	34285
Faulty connection parameters can be cleaned up in the system connection wizard.	34367
A new consistency check tests whether the system connection is writable when **Correct rogue modifications** is set on a property mapping rule.	34576
Improved display of messages in the synchronization log.	34691
Improved display of the origin of Azure Active Directory subscriptions and service plans for employees.	32744
Improved documentation of the features, recommendations, and necessary modifications when operating an Azure Active Directory federation.	33378
Improved support for linking Azure Active Directory user accounts and Active Directory user accounts in an Azure Active Directory federation.	34051
Improved handling of Azure Active Directory group owners when deleting groups.	33653
LDAP containers can be renamed.	34134
The syntax rules for LDAP attributes are now displayed in the Synchronization Editor in addition to the descriptions.	33434

Enhancement	Issue ID
Improved handling of multi-forest structures when resolving the DNS of the Global Catalog. The algorithm for searching the Global Catalog now takes the Active Directory forest root domain into account when searching.	31179
Improved display of Active Directory objects in the Manager and in reports. The full domain name (ADSDomain.ADSDomainName) is now used.	32242
The member schema properties of Active Directory groups is read-only in the target system browser to prevent write accesses that would lead to incorrect results if a group has more than 1500 members. A patch for synchronization projects with patch ID VPR#34324 is provided.	34324
Improved support for dynamic groups in Active Directory.	34769, 34632
Improved logging in the Active Roles connector.	33801
Improved treatment of dynamic groups in Active Roles.	34287, 34323, 34627
The Microsoft Exchange policy for mobile email queries has been renamed to **Mobile device mailbox policy**.	27741
The label of the PAGAccessOrder.ValidDurationMinutes column has been changed to **Checkout duration [min]**.	34678
A wait step has been added to the processes ADS_ADSDomain_Publish ADSGroups to ITShop_PostSync and AAD_AADOrganization_Publish AAD objects to ITShop_PostSync to check if the respective process for automatically assigning employees to user accounts (ADS_ADSDomain_SearchandCreate_Person_PostSync and AAD_Organization_SearchAndCreate_Person_PostSync) has finished.	34651, 34658
In the system connection wizard for cloud applications, a reference time zone can be stored for handling date values without UTC offset. A patch for synchronization projects with patch ID VPR#33978 is provided.	33978
The generic database connector for the generic ADO.NET provider now supports reading back automatically mapped value.	34104
Improved logging in the generic database connector.	34823
Improved support for dynamic groups in custom target systems.	34632
Additional reports are provided about user accounts and groups in all target systems.	33456, 33599
Various reports now also show the origin of a membership or entitlement.	27414

Enhancement	Issue ID
Additional access control settings for Google Workspace groups are mapped. A patch for synchronization projects with patch ID VPR#32610 is provided.	32610
The HROrgUnitManager schema type has been extended so that the validity period of manager assignments can now also be mapped.	33209
The default company of SAP clients can now be read in by the synchronization. A patch for synchronization projects with patch ID VPR#33819 is provided.	33819
For target systems in Unified Namespace, an overview form is displayed in the Manager.	33412
The overview form for E-Business Suite systems (VI_EBS_EBSSystem_Overview) displays a message if no synchronization project has been set up.	34380
The Windows PowerShell connector and the One Identity Safeguard connector now treat passwords as secret values. A patch for synchronization projects with patch ID VPR#34403 is provided.	34403
The edsaIsDynamicGoup property of Active Directory groups is mapped in One Identity Manager. A patch for synchronization projects with patch ID VPR#34168 is provided.	34168
Additional schema properties are mapped to Google Workspace user accounts. A patch for synchronization projects with patch ID VPR#33093 is provided.	33093
The SCIM connector now allows parallel access 10 times max. to load single objects during synchronization. A patch for synchronization projects with patch ID VPR#32564 is provided.	32564
When using Universal Cloud Interface to synchronize cloud applications, it is now possible to configure whether to keep the target system connected. A patch for synchronization projects with patch ID VPR#33884 is provided.	33884

Table 4: Identity and Access Governance

Enhancement	Issue ID
Additional permitted values for Person.ImportSource.	24169
For automatic approvals of requests and attestation cases the following now applies: If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. Additional approvers must grant or deny approval within the time period that applied to the previous approvers.	33182

Enhancement	Issue ID
User accounts that are intentionally not assigned an employee can be marked accordingly. If attestation of user accounts that are not connected with an employee is approved, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not connected with an identity can be filtered by different categories.	33384, 34387
Text templates describing the facts to be attested can be stored in attestation procedures. This text is displayed to attestors in the Web Portal.	33494
Improved performance when setting up attestation cases and attestation runs.	33742, 34017, 34039, 34202, 34217, 34243, 34344, 34431
Attestation policies can have an application role assigned as the owner, so multiple employees can own an attestation policy.	33783
Attestation guidelines can define the language in which to display the information to be attested.	34148
Additional reports on attestation runs are provided, which contain the complete attestation history.	34203
Customized reports can now be assigned to default attestation procedures.	34569
Mail templates used for notifying rule and policy supervisors and exception approvers are now directly mapped to compliance rules and company policies. The following configuration parameters have been deleted: • QER | Policy | EmailNotification | NewExceptionApproval • QER | Policy | EmailNotification | NotPermittedViolation • QER | ComplianceCheck | EmailNotification | NewExceptionApproval • QER | ComplianceCheck | EmailNotification | NotPermittedViolation When the One Identity Manager database is updated, the values of the configuration parameters are transferred to the new `ComplianceRule.UID_DialogRichMailNewViolation` and `QERPolicy.UID_DialogRichMailNewViolation` columns.	31781
Approval steps can now be escalated even if no approver or attestor can be determined and no fallback approver is assigned. In this case, the request or attestation case is no longer canceled or passed on to the chief approval team, but escalated.	27902

Enhancement	**Issue ID**
The **CM** approval procedure can now also be used to attest system role assignments and employee's account definitions.	34290
When sending email notifications in the IT Shop and attesting, the sender address entered at the **QER | Attestation | DefaultSenderAddress** and **QER | ITShop | DefaultSenderAddress** configuration parameters is now given by default. The employee's default email address is no longer used as the sender address for automatic notifications.	32072
Permissions for the **Request & Fulfillment | IT Shop | Administrators** application role have been extended.	32185
On the overview forms of departments, locations, cost centers, business roles, application roles, and IT Shop structures, existing delegations of the manager and 2. manager are displayed.	32682
Improved performance when saving requests.	33898
New consistency check **Direct memberships in BaseTree that are not allowed** to identify direct assignments to roles and organizations for which direct assignment is not allowed.	34060
Recalculation of a dynamic role can be temporarily disabled (`DynamicGroup.IsRecalculationDeactivated`).	34076
Using the `@UID_Org` variable, you can access the role or organization referenced by the dynamic role.	33757, 31554
Improved calculation of dynamic rolls.	29973
The usage type of standard reasons can now be edited by users.	34218
The configuration parameters for automatic transfer of groups to the IT Shop have been restructured. The previous **QER | ITShop | GroupAutoPublish** configuration parameter and the preprocessor expression `GroupAutoPublish` applied to Active Directory and SharePoint groups. This has been divided up. The `GroupAutoPublish` preprocessor expression is still used with the new **QER | ITShop | AutoPublish | ADSGroup** configuration parameter. For the new **QER | ITShop | AutoPublish | SPSGroup** configuration parameter, the preprocessor expression `AutoPublish_SPSGroup` has been introduced. NOTE: If you have implemented customizations for SharePoint groups that use the `GroupAutoPublish` preprocessor expression, then change the preprocessor expression to `AutoPublish_SPSGroup` for this.	34310
Additional properties can now also be assigned to LDAP containers.	34401
Improved preparation of data for faster cross-table searching. It is now possible to additionally specify a path to the Person object in order to	31167

Enhancement	Issue ID
determine the employee within the cross-table search for user accounts or email addresses.	
When automatically creating application roles for product owners, the display name of the person is now used to form the application role name.	34602
When submitting requests, the valid until date is no longer checked against the current time. For example, errors are avoided if a long time has elapsed between creating and sending a shopping cart.	34621

See also:

- Schema changes on page 42
- Patches for synchronization projects on page 62

Resolved issues

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

Table 5: General

Resolved issue	Issue ID
Parameter values are not copied entirely from the process simulation to the clipboard.	32724
Blockage when running `QBM_PProcessGroupDelete` while transferring data to the History Database.	34796
The `DateRange` class static methods do not yet perform the time zone conversion properly.	33009
Object definitions (`DialogObject`) can be created without a table reference.	33155
Error in the Schema Editor when editing tables and columns.	33429
Dates with the time 0:00 are not correctly converted to UTC format.	33472
It is not possible to create databases with a name longer than 40 characters.	33549, 33906
High memory consumption when compiling with the Configuration Wizard or the Database Compiler.	33563
Automatic software update does not take the files only option into account.	34454
When process steps with the **Frozen** status in Job Queue Info are advanced,	34496

Resolved issue	Issue ID
the subsequent process step loses its retries.	
A change to the **UseSSL** option in the One Identity Manager Service configuration requires a restart of the service, although this is not necessary according to the information displayed in the Job Service Configuration.	34525
Error in the `QBM_PDBQueueRunner` procedure when removing modules.	34555
Error logging in to the Manager web application with Japanese language.	34558
When testing whether a report contains data, an error may occur. Error message: `Could not find stored procedure 'Report_LimitData'.`	34596
Entering a string for an event's process data results in a compilation error. Error message: `'<text>' is not declared. It may be inaccessible due to its protection level.`	34716
Data provided by the application server does not fill foreign keys with a **NULL** but an empty string.	34720
Error in Schema Extension when creating a custom table with a foreign key to a `Basetree*` view.	34749
Error in the **DialogDeferredOperation with overdue actions, activated but without existing job** consistency check.	34765
The `QER_TIPersonInBaseTree` trigger for checking `BaseTreeExcludesBaseTree violations` does not take the `XOrigin` column into account.	34519
When generating a preview for simple list reports, errors may occur under certain circumstances.	34752
Reports no longer correctly hide the minimum date (12/30/1899).	34550
A system user who has read-only permissions may be given additional change permissions by program functions.	34812
If a user account password is changed, the Customizer throws an error if the change is discarded rather than saved.	33594
Error in the **Missing tables in dialogtable (base)** consistency check's repair script.	34846
When saving formation rules in the System Debugger, the code disappears if there is a `<summary>` section in the code.	34404
Templates are not booked to the change label when saved to the System Debugger.	34412
Translations do not take all language dependencies into account.	34410

Resolved issue	Issue ID
In certain circumstances, `DialogWatchOperation.OperationUser` is not be populated.	34429
Error opening the TimeTrace in the Manager.	34449

Table 6: General web applications

Resolved issue	Issue ID
The **New child group** button contains the **CanInsert("AdsGroup")** viewing condition. This viewing condition has been removed.	34544
The following collections have been removed from the **VI_ITShop_Approvals** Web Designer component: - ITShopOrg - ITShopOrgForPWOToDecide - PWOHelperPWO - QERWorkingStep - PWOHelperPWOForRecallQuery The **ITShopOrg** collection was removed from the **VI_ITShop_PWO_MasterDetail** component.	201868
In the Web Portal, the reason stored is incorrect if products are automatically canceled due to denied attestation.	202027
In certain circumstances in the Web Portal, an attestation case approver cannot analyze the removal of permissions.	202031
In the Operations Support Web Portal users can create passcodes for themselves.	202046
In the Web Designer Web Portal it is possible to display hyperviews for which you do not have required permissions.	223719
The API Server cannot be installed because a WebDAV module is installed on the same Internet Information Services.	227123
If you search for AE/Ä in the Web Portal, entries with A are also found. NOTE: Perform a complete re-indexing after an update migration.	278865, 34389
In the Web Portal it ASP.NET sessions can go missing if Linux containers are in continuous operation.	34397
In the Web Portal, identities with the **vi_4_PERSONADMIN** permissions group do not see all the requests of their child identities.	33773
In the Web Portal, if a cancellation date that is in the past is specified for a	34144

Resolved issue	Issue ID
cancellation, an error message appears. Subsequently, the product cannot be canceled even with a valid date.	
In the Web Portal, it is not possible to resolve compliance violations if the violation involves a primary identity.	34416

Table 7: Target system connection

Resolved issue	Issue ID
Mappings that have the **Only suitable for updates** option enabled use the `Insert` processing method. Patches with the patch IDs VPR#33217_001 and VPR#33217_002 are available for synchronization projects.	33217
Too many entries are logged when detecting and correcting invalid changes.	34439
Synchronization stopped due to an error synchronizing with revision filtering: The revision property type does not match. Error message: `Error filtering by revision. ---> System.ArgumentException: Object must be of type Int32.`	34462
Error compiling scripts in C# syntax in Synchronization Editor, if an assignment is missing a space after the equals sign (**=**).	34500
Error creating a synchronization project with the `SynchronizationEditor.CLI.exe` command line utility if the database user's password contains a dollar sign (**$**).	34531
Error loading schema classes with the **Unique objects** class type using the RemoteConnectPlugin.	34683
Error provisioning the **Password cannot be changed** property for Active Directory user accounts (`ADSAccount.UserCanNotChangePassword`).	34390
Poor performance when opening assignment forms for `ADSAccountInADSGroup`.	34510
The Azure AD Connect anchor ID for Active Directory user accounts (`ADSAccount.MSDsConsistencyGuid`) cannot be overwritten in the map. A patch with the patch ID VPR#34715 is available for synchronization projects.	34715
Error saving an Microsoft Exchange mailbox if the **Calendar Automate Enabled** property (`EX0Mailbox.AutomateProcessing`) is empty.	34610
In the case of automatic employee assignment, for LDAP user accounts the **Groups inheritable** option (`LDAPAccount.IsGroupAccount`) is always set to **True**.	34556
When deleting an LDAP user account, memberships in LDAP groups are not	34594,

Resolved issue	Issue ID
removed if merge mode is active.	34601
Error in the SCIM connector during OAuth authentication with user name and password. Error message: `Error 400 BadRequest ({"error": "invalid_request", "error_description": "The request contains invalid parameters or values."})`	34578
Error running the `EBS_UserInResp` procedure. Error message: `Conversion failed when converting date and/or time from character string`.	34754
In the SAP connector, the `LANGU` property of the `SAPTSAD3T` schema type is not output correctly.	34557
In One Identity Manager, synchronization tries to recreate SAP roles assignments to user accounts with `XIsInEffect=0`. A patch with the patch ID VPR#34563 is available for synchronization projects.	34563
Search criteria for automatic employee assignment with an OR link causes a lots of hits if one of the fields is empty.	34415
If the validity period changes, SAP role assignments to user accounts are temporarily deleted.	34577
Problems synchronizing SharePoint Online when a site collection (`site`) is renamed in the target system.	34471
Defining a hierarchy filter in the scope of the One Identity Manager connection returns the wrong results.	32595
After changing the aliases of a Google Workspace user account, provisioning reloads the old value. A patch for synchronization projects with patch ID VPR#34645 is provided.	34645
During initial synchronization, the internet password is loaded from Notes user accounts. A patch for synchronization projects with patch ID VPR#34393 is provided.	34393
In synchronization projects for Notes domains, the `MailFileAccessType` variable has an incorrect default value. A patch for synchronization projects with patch ID VPR#25230 is provided.	25230
In synchronization projects for Unix-based target systems, the user's password is not encrypted. A patch for synchronization projects with patch ID VPR#32500 is provided.	32500

Table 8: Identity and Access Governance

Resolved issue	Issue ID
Wrong name in bitmask configuration for `PersonHasObject.InheritInfo`.	34721
Querying the origin of entitlements blocks under certain circumstances.	34767
If an employee is deactivated, closed attestation cases are closed again.	34665
The search for specific attestation cases in Web Portal sometimes does not return a result if system entitlements are attested. The reason was the different formatting of display names for the attestation objects. For some tables mapped in Unified Namespace the display pattern has been changed. As a result, these objects are now displayed with different names in reports or views of the Web Portal.	34681
When an approval level with multiple approval steps times out, an identical process is generated multiple times.	34571
Email notifications about granted request approvals name the wrong approver.	34614
A product cannot be requested for several different workstations for which one employee is responsible.	30069

See also:

- Schema changes on page 42
- Patches for synchronization projects on page 62

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

Known Issue	Issue ID
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 Availability Group) and the option `DTC_SUPPORT = PER_DB` is set, replication between the server is done by Distributed Transaction. If a `Save Transaction` is run in the process, an error occurs: `Cannot use SAVE TRANSACTION within a distributed transaction.` Solution: Disable the option `DTC_SUPPORT = PER_DB`.	30972
If no date is given, the date 12/30/1899 is used internally. Take this into account when values are compared, for example, when used in reports. For detailed information about displaying dates and time, see the *One Identity Manager Configuration Guide*.	31322

Known Issue	Issue ID
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 message under the menu explaining the problem. - Add a default schedule to the subscribable report. - In the Web Designer, change the **Filter for subscribable reports** configuration key (**VI_Reporting_Subscription_Filter-RPSSubscription**) and set the schedule's **Minimum character count** value (`UID_DialogSchedule`) to **1**.	32938
If the application is supplemented with custom DLL files, an incorrect version of the `Newtonsoft.Json.dll` file might be loaded. This can cause the following error when running the application:	33867

Known Issue	Issue ID

`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>`	

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

Table 11: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use `Import-PSSession` internally.	23795
By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely. Solution: Make it possible to access the building block **HR_ENTRY_DATE** remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate` in the Synchronization Editor.	25401
Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses were stored up to now.	27042
Error in Domino connector (`Error getting revision of schema type ((Server))`). Probable cause: The HCL Domino environment was rebuilt or numerous	27126

Known Issue	Issue ID
entries have been made in the Domino Directory. Solution: Update the Domino Directory indexes manually in the HCL Domino environment.	
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 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.	29556
Target system synchronization does not show any information in the Manager web application. Workaround: Use Manager to run the target system synchronization.	30271

Known Issue	Issue ID
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 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"`
	32149

Known Issue	Issue ID

`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 Workspace, save a user data transfer XML. In this XML document, limit the list to the user data to be transferred. Only run the Google applications that have user data you still need. For more information and an example XML, see *One Identity Manager Administration Guide for Connecting to Google Workspace*.	33104
In the schema type definition of a schema extension file for the SAP R/3 schema, if a `DisplayPattern` is defined that has another name in the SAP R/3 schema as in the One Identity Manager schema, performance issue may occur. Solution: Leave the `DisplayPattern` empty in the schema type definition. Then the object's distinguished name is used automatically.	33812

Known Issue	Issue ID
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

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	29051

Known Issue	Issue ID
as one page.	
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, if the `boolean` data type is redefined), it can lead to various problems in One Identity Manager.	31998

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

Known Issue	Issue ID
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.	

Schema changes

The following provides an overview of schema changes from version 8.1.5 up to version 8.2.

Microsoft Teams Module

- New data model for the Microsoft Teams Module.

Application Governance Module

- New data model for the Application Governance Module.

Configuration Module

- New table `QBMColumnBitMaskConfig` and new columns `DialogColumn.BitMaskConfigOrder`, `DialogColumn.DisallowCustomBitMaskConfig`, and `DialogColumn.HasBitMaskConfig` for mapping bitmasks.
- New table `QBMColumnLimitedValue` for mapping lists of permitted values.
- New tables `QBMTableRevision` and `QBMVTableRevision` for mapping revision data for tables.
- New table `QBMTrustedSQL` and new column `QBMWebApplication.TrustedSourceKey` for mapping trusted SQL queries.
- New table `QBMVSystemState` to map the system status.
- New column `DialogColumn.MultiValueSpecification` for defining further requirements for the single values of MVP columns.
- New columns `DialogCountry.IsHistorical` and `DialogState.IsHistorical` for marking countries and states as historical.
- New column `DialogDashBoardDef.DashBoardType` to map types of statistics definitions.
- New column `DialogDatabase.UID_DialogCountryDefault` to specify a default country.
- New column `DialogDatabase.UpdatePhase` to map the phases for step-by-step preparation of a migration.

- New column DialogMethod.IsVisibleScript for a script to conditionally show the method.
- New column DialogRichMail.AttachmentFileName as a template for formatting the file name for the report attachment.
- New column DialogTable.DeleteDelayScript for a script to determine an object-specific deferred deletion.
- New column DialogTable.SplittedLookupSupport as path to a Person object for cross-table searching.
- New column DialogTree.HelpKey for mapping a help key.
- New columns for QBMConsistencyCheck.AccessLevelMin, QBMConsistencyCheck.DescriptionElementDetect, and QBMConsistencyCheck.DescriptionRepair for consistency checks.
- New columns QBMDBQueueTask.RestoreDelay and QBMDBQueueTaskPerf.RestoreDelay to map a minimum time until reactivation of DBQueue Processor tasks.
- New columns QBMHtmlApp.Ident_QBMHtmlApp, QBMHtmlApp.IsPreCompiled and QBMHtmlApp.SortOrder for HTML applications.
- New columns QBMIdentityClient.AcrValues and QBMIdentityProvider.AcrValues to map acr values.
- New columns QBMIdentityClient.IsSendPostLogoutRedirectURI and QBMIdentityClient.PostLogoutRedirectURI for forwarding URI details.
- New columns QBMIdentityClient.TokenEndpointCertThumbPrint for the fingerprint of the certificate to verify the token.
- New columns QBMIdentityProvider.CheckClaim and QBMIdentityProvider.CheckValue for checking an additional claim type.
- New column QBMIdentityProvider.NoIdTokenCheck to specify whether the ID token is checked.
- New column QBMLimitedSQL.TypeOfLimitedSQL to specify a type for the predefined SQL.
- New column QBMPwdPolicy.MandatoryCharacterClasses to specify how many rules must be met for character classes.
- New columns QBMServer.FQDNExternaland and QBMServer.PortNumberExternal for accessing Job servers.
- New column for QBMServer.NotUsedForJobCreation to specify whether the Job server participates in load balancing.
- New column QBMUniqueGroup.ViolationMessage to enter error message text.
- New column QBMVSystemOverview.SubElement for better evaluation of the system configuration.
- The data type for the columns DialogColumnBulkDependencies.XTouched, QBMBufferConfig.XTouched, QBMColumnTranslation.XTouched, QBMNonLinearDepend.XTouched, QBMTransportHistory.XTouched, and

QBMUniqueGroupHasColumn.XTouched has been changed to nchar(1).

- The DialogDatabase.ConnectionString column has been extended to nvarchar(max).
- The DialogSchedule.StartTime column has been extended to varchar(256).
- The QBMConsistencyCheck.Description column has been extended to nvarchar(max).
- The columns QBMDBPrincipal.LoginName and QBMDBPrincipal.UserName have been extended to nvarchar(128).
- The QBMDBRoleDef.Rolename column has been extended to nvarchar(400).
- The data type for the QBMFileRevision.HashValue column has been changed to varbinary(64).
- New mandatory field definition for the DialogObject.UID_DialogTable column.
- The QBMVBlobInternal table has been deleted.
- The QBMIdentityClient.TokenEndpointKey column has been deleted.

Target System Synchronization Module

- New tables DPRProjectionDependency and DPRSystemSyncDependency to map dependencies for synchronization.
- New tables DPRVSyncRunMessages and DPRVSyncRunOverview for improved evaluation of synchronization logs.
- New columns for mapping system synchronization.
    - DialogColumn.SystemSyncDirection
    - DialogTable.SystemSyncKeyColumns
    - DialogTable.SystemSyncMode
    - DialogTable.UID_SystemSyncConfigCLRType
    - DPRProjectionConfigStep.DoNotRespectOutstanding
- New column DPRProjectionConfig.JournalMessageContexts for better mapping of journal entries.
- New columns DPRProjectionStartInfo.ProgressText and DPRProjectionStartInfo.ProgressValue for mapping the progress of synchronizations.
- New column DPRRevisionStore.ValueType to map the type of revision value.
- New column DPRSchema.FunctionalLevel for mapping the development state of a schema.
- New column DPRSchemaType.ShrinkLock to prevent removing the schema type during schema compression.
- New column DPRShell.IsAutomaticallyManaged to specify whether the synchronization project is automatically managed.
- New column DPRShell.LastMigrationError to map the error message of the last migration of a synchronization project.

- New column `DPRStartSequence.ConcurrConflHandling` to map the behavior in case of collisions.
- New column `DPRStartSequenceHasProjection.CurrentJobReference` to map the currently running process.
- The `DPRJournal.ProjectionState` column has been extended to `varchar(64)`.
- The `DPRSchemaProperty.AutoFillBehavior` and `DPRSchemaProperty.MandatoryBehavior` columns have been extended to `nvarchar (64)`.

Target System Base Module

- New tables for advanced mapping of system entitlements in cloud target systems.
  - BaseTreeHasUNSGroupB1
  - BaseTreeHasUNSGroupB2
  - BaseTreeHasUNSGroupB3
  - DepartmentHasUNSGroupB1
  - DepartmentHasUNSGroupB2
  - DepartmentHasUNSGroupB3
  - ITShopOrgHasUNSGroupB1
  - ITShopOrgHasUNSGroupB2
  - ITShopOrgHasUNSGroupB3
  - ITShopSrcHasUNSGroupB1
  - ITShopSrcHasUNSGroupB2
  - ITShopSrcHasUNSGroupB3
  - LocalityHasUNSGroupB1
  - LocalityHasUNSGroupB2
  - LocalityHasUNSGroupB3
  - OrgHasUNSGroupB1
  - OrgHasUNSGroupB2
  - OrgHasUNSGroupB3
  - ProfitCenterHasUNSGroupB1
  - ProfitCenterHasUNSGroupB2
  - ProfitCenterHasUNSGroupB3
  - UNSAccountBHasUNSGroupB
  - UNSAccountBHasUNSGroupB1
  - UNSAccountBHasUNSGroupB2
  - UNSAccountBHasUNSGroupB3

  - UNSAccountBInUNSGroupB1
  - UNSAccountBInUNSGroupB2
  - UNSAccountBInUNSGroupB3
  - UNSGroupB1
  - UNSGroupB1Collection
  - UNSGroupB1Exclusion
  - UNSGroupB1InUNSGroupB1
  - UNSGroupB2
  - UNSGroupB2Collection
  - UNSGroupB2Exclusion
  - UNSGroupB2InUNSGroupB2
  - UNSGroupB3
  - UNSGroupB3Collection
  - UNSGroupB3Exclusion
  - UNSGroupB3InUNSGroupB3
- New columns `UNSRootB.GroupUsageMask`, `UNSRootB.UserContainsGroupList`, and `UNSAccountB.XDateSubItem` for advanced mapping of system entitlements in cloud target systems.
- New column `UNSGroupB.HasReadOnlyMemberships` to map dynamic memberships.
- New columns `UNSAccountB.IsGroupAccount_UNSGroupB`, `UNSAccountB.IsGroupAccount_UNSGroupB1`, `UNSAccountB.IsGroupAccount_UNSGroupB2`, and `UNSAccountB.IsGroupAccount_UNSGroupB3` for better mapping of inheritance of groups and permissions.
- New columns `UNSAccountB.IsNeverConnectManual` and `UNSAccountB.NeverConnectToPerson` for mapping connections to employees.
- New column `AERoleHasTSBAccountDef.XIsInEffect` to map the assignments in effect.
- New column `TSBAERoleForRoot.UID_AERoleMemberShip` to map target system members.
- New column `UNSAccountB.XDateSubItem` to map the modification date of dependencies.
- New column `UNSRootB.DeleteDelayDays` to map a delete delay of custom target systems.
- The data type for the `UNSAccountB.MatchPatternForMembership` and `UNSGroupB.MatchPatternForMembership` columns has been changed to `bigint`.
- The data type for the columns `TSBITData.XTouched`, `TSBITDataMapping.XTouched`, `TSBVUNSDomain.XTouched`, and `TSBVUNSRoot.XTouched` has been changed to `nchar(1)`.

Azure Active Directory Module

- New tables AADApplication and AADApplicationOwner for mapping Azure Active Directory applications.
- New tables AADServicePrincipal and AADServicePrincipalOwner to map Azure Active Directory service principals.
- New tables AADAppRole and AADAppRoleAssignment to map app roles.
- New tables AADGroupHasDeniedService, AADGroupHasSubSku, and AADUserHasSubSkuCompressed to map license assignments across Azure Active Directory groups.
- New tables AADHomeRealmDiscoveryPolicy, AADServicePrincipalOwner, AADTokenIssuancePolicy, and AADTokenLifetimePolicy to map Azure Active Directory policies.
- New columns for mapping additional properties of Azure Active Directory user accounts.
  - AADUser.AboutMe
  - AADUser.AgeGroup
  - AADUser.BirthDay
  - AADUser.ConsentProvidedForMinor
  - AADUser.EmployeeID
  - AADUser.FaxNumber
  - AADUser.HireDate
  - AADUser.ImAddresses
  - AADUser.Interests
  - AADUser.IsResourceAccount
  - AADUser.LegalAgeGroupClassification
  - AADUser.MySite
  - AADUser.OnPremisesDistinguishedName
  - AADUser.OnPremisesDomainName
  - AADUser.OnPremisesExtensionAttribute1
  - AADUser.OnPremisesExtensionAttribute10
  - AADUser.OnPremisesExtensionAttribute11
  - AADUser.OnPremisesExtensionAttribute12
  - AADUser.OnPremisesExtensionAttribute13
  - AADUser.OnPremisesExtensionAttribute14
  - AADUser.OnPremisesExtensionAttribute15
  - AADUser.OnPremisesExtensionAttribute2

  - AADUser.OnPremisesExtensionAttribute3
  - AADUser.OnPremisesExtensionAttribute4
  - AADUser.OnPremisesExtensionAttribute5
  - AADUser.OnPremisesExtensionAttribute6
  - AADUser.OnPremisesExtensionAttribute7
  - AADUser.OnPremisesExtensionAttribute8
  - AADUser.OnPremisesExtensionAttribute9
  - AADUser.OnPremisesSAMAccountName
  - AADUser.OnPremisesUserPrincipalName
  - AADUser.OtherMails
  - AADUser.PastProjects
  - AADUser.PreferredName
  - AADUser.Responsibilities
  - AADUser.Schools
  - AADUser.Skills
- New columns `AADUser.ExternalUserState` and `AADUser.ExternalUserStateChangeDate` for mapping guest users.
- New columns `AADUser.NeverConnectToPerson` and `AADUser.IsNeverConnectManual` for mapping connections to employees.
- New columns `AADUser.IsGroupAccount_DeniedService`, `AADUser.IsGroupAccount_DirectoryRole`, `AADUser.IsGroupAccount_Group` and `ADUser.IsGroupAccount_SubSku` for better mapping of inheritance of groups and permissions.
- New column `AADUser.LastPasswordChangeDateTime` to map the date of the last password change.
- The data type for the columns `AADDeniedServicePlan.MatchPatternForMembership`, `AADDirectoryRole.MatchPatternForMembership`, `AADGroup.MatchPatternForMembership`, `AADSubSku.Match PatternForMembership`, and `AADUser.Match PatternForMembership` has been changed to `bigint`.
- The mandatory field definition for the `AADUser.DisplayName` and `AADUser.UserPrincipalName` columns has been changed.
- The table `AADSubSkuExclusion` has been deleted.
- The columns `AADUserHasSubSku.RiskIndexCalculated` and `AADUserHasSubSku.UID_AADSubSku` have been deleted.

Exchange Online Module

- New column `AADUser.IsGroupAccount_UnifiedGroup` for better mapping of inheritance of groups and permissions.

- New columns O3EMailbox.UID_Person, O3EMailbox.IsNeverConnectManual, O3EMailbox.NeverConnectToPerson, O3EMailContact.IsNeverConnectManual, O3EMailContact.NeverConnectToPerson, O3EMailUser.IsNeverConnectManual, and O3EMailUser.NeverConnectToPerson to map connections to employees.
- New column O3EUnifiedGroup.HiddenFromExchClientsEnabled to hide the Office 365 group in Outlook.
- The data type for the columns O3EDL.MatchPatternForMembership, O3EMailbox.MatchPatternForMembership, O3EMailContact.MatchPatternForMembership, O3EMailUser.MatchPatternForMembership, and O3EUnifiedGroup.MatchPatternForMembership has been changed to bigint.
- The data type for the O3EMailbox.XTouched column has been changed to nchar(1).

Active Directory Module

- New columns ADSAccount.IsNeverConnectManual, ADSAccount.NeverConnectToPerson, ADSContact.IsNeverConnectManual, and ADSContact.NeverConnectToPerson for mapping connections to employees.
- New columns ADSAccount.IsProtectedFromAccidentalDel, ADSContact.IsProtectedFromAccidentalDel, ADSGroup.IsProtectedFromAccidentalDel, and ADSMachine.IsProtectedFromAccidentalDel to protect against accidental deletion.
- New columns ADSContact.MSDsConsistencyGuid, ADSGroup.MSDsConsistencyGuid, and ADSMachine.MSDsConsistencyGuid to map Azure AD Connect anchor ID.
- New column ADSAccount.MiddleName to map the middle name.
- New column ADSGroup.HasReadOnlyMemberships to map dynamic memberships.
- The data type for the ADSAccount.MatchPatternForMembership, ADSContact.MatchPatternForMembership, and ADSGroup.MatchPatternForMembership columns has been changed to bigint.

Active Roles Module

- New column ADSGroup.edsaIsDynamicGroup for mapping dynamic groups.
- New columns ADSGroup.edsvaCGisControlledGroup and ADSGroup.edsvaGFIsGroupFamily for mapping Active Roles Group Family groups.

Microsoft Exchange Module

- New table EX0AddrBookPolicy and new column EX0MailBox.UID_EX0AddrBookPolicy to map Microsoft Exchange address book policies.
- New tables EX0MailboxFullAccessPerm and EX0MailboxSendAsPerm for mapping additional Microsoft Exchange mailbox permissions.
- New columns EX0MailBox.IsNeverConnectManual, EX0MailBox.NeverConnectToPerson, EX0MailContact.IsNeverConnectManual, EX0MailContact.NeverConnectToPerson,

EX0MailUser.IsNeverConnectManual, and EX0MailUser.NeverConnectToPerson for mapping connections to employees.

- New column EX0MailBox.IsSingleItemRecoveryEnabled for single item recovery.
- New columns EX0MailBoxDatabase.IsExcludedFromProvisioning and EX0MailBoxDatabase.IsSuspendedFromProvisioning to map automatic mailbox distribution for Microsoft Exchange mailbox databases.
- The data type for the columns EX0DL.XTouched, EX0DynDL.XTouched, EX0MailBox.XTouched, and EX0Server.XTouched has been changed to nchar(1).

Exchange Hybrid Module

- New columns EXHRemoteMailbox.IsNeverConnectManual and EXHRemoteMailbox.NeverConnectToPerson for mapping connections to employees.

LDAP Module

- New columns LDAPAccount.IsNeverConnectManual and LDAPAccount.NeverConnectToPerson for mapping connections to employees.
- The data type for the LDAPAccount.MatchPatternForMembership and LDAPGroup.MatchPatternForMembership columns has been changed to bigint.
- The LDPDomain.Ident_Domain column has been extended to nvarchar(128).

Unix Based Target Systems Module

- New columns UNXAccount.IsNeverConnectManual and UNXAccount.NeverConnectToPerson for mapping connections to employees.
- The data type for the UNXAccount.MatchPatternForMembership and UNXGroup.MatchPatternForMembership columns has been changed to bigint.

Oracle E-Business Suite Module

- New columns EBSUser.IsNeverConnectManual and EBSUser.NeverConnectToPerson for mapping connections to employees.
- The data type for the columns EBSUser.MatchPatternForMembership and EBSResp.MatchPatternForMembership has been changed to bigint.

Domino Module

- New columns NDOUser.IsNeverConnectManual and NDOUser.NeverConnectToPerson to map connections to employees.
- The data type for the NDOUser.MatchPatternForMembership and NDOGroup.MatchPatternForMembership columns has been changed to bigint.

SharePoint Module

- New columns `SPSUser.IsGroupAccount_SPSGroup` and `SPSUser.IsGroupAccount_SPSRLAsgn` for better mapping of inheritance of groups and permissions.
- New columns `SPSUser.IsNeverConnectManual` and `SPSUser.NeverConnectToPerson` for mapping connections to employees.
- The data type for the `SPSUser.MatchPatternForMembership`, `SPSRLAsgn.MatchPatternForMembership`, and `SPSGroup.MatchPatternForMembership` columns has been changed to `bigint`.

SharePoint Online Module

- New table `O3SWebTemplate` for mapping SharePoint Online web templates.
- New columns `O3SUser.IsGroupAccount_Group` and `O3SUser.IsGroupAccount_RLAsgn` for better mapping of inheritance of groups and permissions.
- New columns `O3SUser.IsNeverConnectManual` and `O3SUser.NeverConnectToPerson` for mapping connections to employees.
- New columns `O3SSite.UserCodeWarningLevel` to map additional thresholds for SharePoint Online site collections.
- The data type for the columns `O3SUser.MatchPatternForMembership`, `O3SRLAsgn.MatchPatternForMembership`, and `O3SGroup.MatchPatternForMembership` has been changed to `bigint`.

Google Workspace Module

- New tables to map assignments of Google Workspace admin roles.
  - DepartmentHasGAPOrgAdminRole
  - GAPBaseTreeHasOrgAdminRole
  - ITShopOrgHasGAPOrgAdminRole
  - ITShopSrcHasGAPOrgAdminRole
  - LocalityHasGAPOrgAdminRole
  - OrgHasGAPOrgAdminRole
  - ProfitCenterHasGAPOrgAdminRole
- New columns to map assignments of Google Workspace admin roles.
  - GAPOrgAdminRole.DisplayName
  - GAPOrgAdminRole.IsForITShop
  - GAPOrgAdminRole.IsITShopOnly
  - GAPOrgAdminRole.MatchPatternForMembership
  - GAPOrgAdminRole.RiskIndex
  - GAPOrgAdminRole.UID_AccProduct

    - GAPUserInOrgAdminRole.RiskIndexCalculated
    - GAPUserInOrgAdminRole.XIsInEffect
    - GAPUserInOrgAdminRole.XOrigin
- New columns `GAPUser.IsGroupAccount_Group`, `GAPUser.IsGroupAccount_OrgAdminRole`, and `GAPUser.IsGroupAccount_PaSku` for better mapping of inheritance of groups and permissions.
- New columns `GAPUser.IsNeverConnectManual` and `GAPUser.NeverConnectToPerson` for mapping connections to employees.
- New columns for mapping additional properties for Google Workspace user accounts.
    - GAPUser.GenderAddressMeAs
    - GAPUser.GenderCustomGender
    - GAPUser.GenderType
    - GAPUser.RecoveryEmail
    - GAPUser.RecoveryPhone
- New columns for mapping additional properties for Google Workspace groups.
    - GAPGroup.stWhoCanContactOwner
    - GAPGroup.stWhoCanDiscoverGroup
    - GAPGroup.stWhoCanModerateContent
    - GAPGroup.stWhoCanModerateMembers
    - GAPGroup.stWhoCanViewGroup
    - GAPGroup.stWhoCanViewMembership
- The data type for the columns `GAPGroup.MatchPatternForMembership`, `GAPPaSku.MatchPatternForMembership`, and `GAPUser.MatchPatternForMembership` has been changed to `bigint`.
- The columns `GAPGroup.stAllowGoogleCommunication` and `GAPGroup.stShowInGroupDirectory` have been deleted.

SAP R/3 User Management module Module

- New columns `SAPUser.IsGroupAccount_SAPGrp`, `SAPUser.IsGroupAccount_SAPProfile` and `SAPUser.IsGroupAccount_SAPRole` for better mapping of inheritance of groups and permissions.
- New columns `SAPUser.IsNeverConnectManual` and `SAPUser.NeverConnectToPerson` for mapping connections to employees.
- New column `SAPUser.IdAdType` for mapping user types.
- New columns for mapping additional properties for SAP user accounts.
    - SAPUser.BirthName
    - SAPUser.FirstName2

  - SAPUser.LastName2
  - SAPUser.NameAddOn
  - SAPUser.NameAddOn2
  - SAPUser.SORT1
  - SAPUser.SORT2
- The data type for the columns SAPGroup.MatchPatternForMembership, SAPGrp.MatchPatternForMembership, SAPProfile.MatchPatternForMembership, SAPRole.MatchPatternForMembership, and SAPUser.MatchPatternForMembership has been changed to bigint.

SAP R/3 Compliance Add-on Module

- New table SACTransactionType and new columns SAPTransaction.UID_SACTransactionType and SAPFunctionDetail.UID_SACTransactionType to map SAP application types.
- New columns for mapping additional properties for function definition.
  - SAPFunctionDetail.AUTHOBJNAM
  - SAPFunctionDetail.AUTHOBJTYP
  - SAPFunctionDetail.AUTHPGMID
  - SAPFunctionDetail.RFC_NAME
  - SAPFunctionDetail.RFC_TYPE
  - SAPFunctionDetail.SAPHashValue
  - SAPFunctionDetail.SRV_NAME
  - SAPFunctionDetail.SRV_TYPE
  - SAPFunctionDetail.TCD
- New columns for mapping additional properties for SAP applications.
  - SAPTransaction.AUTHOBJNAM
  - SAPTransaction.AUTHOBJTYP
  - SAPTransaction.AUTHPGMID
  - SAPTransaction.RFC_NAME
  - SAPTransaction.RFC_TYPE
  - SAPTransaction.SAPHashValue
  - SAPTransaction.SimpleCompareProperty
  - SAPTransaction.SRV_NAME
  - SAPTransaction.SRV_TYPE
  - SAPTransaction.TCD

    - SAPTransaction.TransactionDisplay
    - SAPFunctionInstanceDetail.UID_SAPTransaction
- The columns `SAPFunctionDetail.TransactionCode`, `SAPFunctionInstanceDetail.TransactionCode`, and `SAPTransaction.Ident_SAPTransaction` have been deleted.

SAP R/3 Structural Profiles Add-on Module

- New column `SAPUser.IsGroupAccount_SAPHRP` for better mapping of inheritance of groups and permissions.
- The data type for the `SAPHRP.MatchPatternForMembership` column has been changed to `bigint`.

Privileged Account Governance Module

- New columns to map access requests for SSH keys for One Identity Safeguard.
    - PAGAsset.SSHHostKeyFingerPrint
    - PAGAsset.SSHKeyProfileName
    - PAGAstAccount.AllowSSHKeyRequest
    - PAGAstAccount.HasSSHKey
    - PAGAstAccount.SSHKeyProfileName
    - PAGUserAttestation.AllowSSHKeyRequest
- New column `PAGUser.AllowPersonalAccounts` to support the vault for personal passwords.
- New columns `PAGUser.IsNeverConnectManual` and `PAGUser.NeverConnectToPerson` for mapping connections to employees.
- The data type for the columns `PAGUser.MatchPatternForMembership` and `PAGUsrGroup.MatchPatternForMembership` has been changed to `bigint`.
- The data type for the following columns has been changed to `nchar(1)`.
    - PAGAccessOrder.XTouched
    - PAGAccGroup.XTouched
    - PAGAccGroupHasMember.XTouched
    - PAGAppliance.XTouched
    - PAGAsset.XTouched
    - PAGAssetInAstGroup.XTouched
    - PAGAstAccount.XTouched
    - PAGAstGroup.XTouched
    - PAGDirAccount.XTouched
    - PAGDirectory.XTouched

  - PAGEntl.XTouched
  - PAGEntlHasMember.XTouched
  - PAGIdentityProvider.XTouched
  - PAGReqPolicy.XTouched
  - PAGReqPolicyApprover.XTouched
  - PAGReqPolicyHasDirAccount.XTouched
  - PAGReqPolicyReviewer.XTouched
  - PAGReqPolicyScopeItem.XTouched
  - PAGUser.XTouched
  - PAGUserAttestation.XTouched
  - PAGUserHasDirAccount.XTouched
  - PAGUserInUsrGroup.XTouched
  - PAGUsrGroup.XTouched

Cloud Systems Management Module

- New tables for advanced mapping of system entitlements in cloud target systems.
  - CSMBaseTreeHasGroup1
  - CSMBaseTreeHasGroup2
  - CSMBaseTreeHasGroup3
  - CSMGroup1
  - CSMGroup1Collection
  - CSMGroup1Exclusion
  - CSMGroup1InGroup1
  - CSMGroup2
  - CSMGroup2Collection
  - CSMGroup2Exclusion
  - CSMGroup2InGroup2
  - CSMGroup3
  - CSMGroup3Collection
  - CSMGroup3Exclusion
  - CSMGroup3InGroup3
  - CSMUserHasGroup
  - CSMUserHasGroup1
  - CSMUserHasGroup2

  - CSMUserHasGroup3
  - CSMUserInGroup1
  - CSMUserInGroup2
  - CSMUserInGroup3
  - DepartmentHasCSMGroup1
  - DepartmentHasCSMGroup2
  - DepartmentHasCSMGroup3
  - ITShopOrgHasCSMGroup1
  - ITShopOrgHasCSMGroup2
  - ITShopOrgHasCSMGroup3
  - ITShopSrcHasCSMGroup1
  - ITShopSrcHasCSMGroup2
  - ITShopSrcHasCSMGroup3
  - LocalityHasCSMGroup1
  - LocalityHasCSMGroup2
  - LocalityHasCSMGroup3
  - OrgHasCSMGroup1
  - OrgHasCSMGroup2
  - OrgHasCSMGroup3
  - ProfitCenterHasCSMGroup1
  - ProfitCenterHasCSMGroup2
  - ProfitCenterHasCSMGroup3
- New columns `CSMRoot.GroupUsageMask` and `CSMRoot.UserContainsGroupList` for advanced mapping of system entitlements in cloud target systems.
- New columns `CSMUser.IsGroupAccount_CSMGroup`, CSMUser. `IsGroupAccount_CSMGroup1`, `CSMUser.IsGroupAccount_CSMGroup2`, and `CSMUser.IsGroupAccount_CSMGroup3` for better mapping of group inheritance and permissions.
- New columns `CSMUser.NeverConnectToPerson` and `CSMUser.IsNeverConnectManual` for mapping connections to employees.
- New column `CSMRoot.DeleteDelayDays` to map a delete delay for cloud target systems.
- The data type for the `CSMUser.MatchPatternForMembership` and `CSMGroup.MatchPatternForMembership` columns has been changed to `bigint`.

Universal Cloud Interface Module

- New tables for advanced mapping of system entitlements in cloud target systems.
    - UCIGroup1
    - UCIGroup1InGroup1
    - UCIGroup2
    - UCIGroup2InGroup2
    - UCIGroup3
    - UCIGroup3InGroup3
    - UCIUserHasGroup
    - UCIUserHasGroup1
    - UCIUserHasGroup2
    - UCIUserHasGroup3
    - UCIUserInGroup1
    - UCIUserInGroup2
    - UCIUserInGroup3
- New columns `UCIRoot.GroupUsageMask` and `UCIRoot.UserContainsGroupList` and `UCIUser.XDateSubItem` for advanced mapping of system entitlement in cloud target systems.

Identity Management Base Module

- New tables `QERPickCategory` and `QERPickedItem` for sample attestation.
- New table `DynamicGroupHasImmediateColumn` and new columns DynamicGroup `.IsCalculateImmediately` and `DynamicGroup.IsRecalculationDeactivated` for improved calculation of dynamic roles.
- New table `QERDynamicGroupBlackList` for mapping exclusion lists for dynamic roles.
- New table `QERBufferRecalcDecisionMaker` for improved calculation of approvers.
- New table `QERITShopOwnerUsage` for mapping product owners.
- New tables `QERUniversalSubstitute` and `QERUniversalSubstituteInRoot` for improved mapping of delegations.
- New tables `QERVBaseTreeHasElement` and `QERVPersonHasElement` to summarize assignments.
- New table `QERVFirstUnicodeChar` to improve grouping and filtering of objects by name.
- New columns to map an application role for managers of company structures.
    - AERole.UID_AERoleManager
    - BaseTree.UID_AERoleManager
    - Department.UID_AERoleManager

    - ITShopOrg.UID_AERoleManager
    - ITShopSrc.UID_AERoleManager
    - Locality.UID_AERoleManager
    - ProfitCenter.UID_AERoleManager
- New columns for mapping approval reasons.
    - AccProduct.ApproveReasonType
    - AccProduct.DenyReasonType
    - AccProduct.OrderReasonType
    - AccProductGroup.ApproveReasonType
    - AccProductGroup.DenyReasonType
    - AccProductGroup.OrderReasonType
    - PWODecisionStep.ApproveReasonType
    - PWODecisionStep.DenyReasonType
- New column `AccProductParamCategory.IsOldStyle` to specify whether the obsolete definition is used for the request parameter of this request property.
- New columns `QERWorkingStep.EscalateIfNoApprover` and `PWODecisionStep.EscalateIfNoApprover` for improved escalation.
- New column `PersonWantsOrg.UiOrderState` to display the request status in the Web Portal.
- New column `PWODecisionRuleRulerDetect.SQLQueryObjectsToRecalc` for improved recalculation of approvers.
- New column `AERoleHasQERResource.XIsInEffect` to map the assignments in effect.
- New columns `OrgRoot.IsPersonAssignOnce` and `OrgType.IsPersonAssignOnce` to prevent assigning people to multiple company structures.
- New column `Person.DecentralizedIdentifier` to map a decentralized identity.
- New column `Person.IsPwdResetByHelpdeskAllowed` to specify whether password resetting by password help desk staff is allowed.
- New columns `QERAssign.IsMAllAssign`, `ShoppingCartItem.ObjectKeyElementUsedInAssign`, and `ShoppingCartItem.ObjectKeyOrgUsedInAssign` to support assignment requests for resources.
- The `QERAssign.Ident_QERAssign` column has been extended to `nvarchar(256)`.
- The data type of the `PersonPasswordHistory.XTouched` column has been changed to `nchar(1)`.

Attestation Module

- New columns `AttestationCase.IsUnderConstruction` and `AttestationRun.CountChunksUnderConstruction` to flag that the attestation case is not yet completely set up.

- New columns AttestationObject.UiText, AttestationObject.UiTextGrouped1, AttestationObject.UiTextGrouped2 and AttestationObject.UiTextGrouped3 to map text templates for attestation procedures.
- New columns AttestationPolicy.IsSetApprovalStateOnApproved and AttestationPolicy.IsSetApprovalStateOnDenied to automatically set the certification status.
- New column AttestationPolicy.IsShowElementsInvolved to show the objects to be attested.
- New column AttestationPolicy.UID_DialogCulture to map the language in which information to be attested is displayed.
- New AttestationPolicy.UID_AERoleOwner column to map an application role whose members are allowed to edit the attestation policy.
- New columns AttestationPolicy.UID_QERPickCategory and AttestationWizardParm.UID_DialogTablePickCategory for sample attestation.

Compliance Rules Module

- New ComplianceRule.UID_DialogRichMailNewViolation column for the new rule violation mail template.
- New columns PersonInNCHasMControl.IsInActive and PersonInNCHasMControl.UID_PersonWantsOrg to improve assignment of mitigating controls when approving requests.

Company Policies Module

- New column QERPolicy.UID_DialogDashBoardDef to map policy violation statistics.
- New column QERPolicy.UID_DialogReport to map policy violations reports.
- New column QERPolicy.UID_DialogRichMailNewViolation for the new policy violation mail template.

Business Roles Module

- New column Org.UID_AERoleManager to map an application role for business role managers.

Report Subscription Module

- New column AERoleHasRPSReport.XIsInEffect to map the assignments in effect.

Changes to system connectors

The following provides an overview of the modified synchronization templates and an overview of all patches supplied by One Identity Manager version 8.1.5 to version 8.2. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 88.

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 62.

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	changed
Active Roles Module	Synchronize Active Directory domain via Active Roles	changed
Cloud Systems Management Module	Universal Cloud Interface synchronization	none
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	changed
	Oracle E-Business Suite CRM data	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)	changed
	Microsoft Exchange 2010 synchronization (v2)	changed
Google Workspace Module	Google Workspace synchronization	changed

Module	Synchronization template	Type of modification
LDAP Module	AD LDS synchronization	changed
	AD LDS Synchronization (version 2)	new
	OpenDJ synchronization	changed
	OpenDJ Synchronization (version 2)	new
	Generic LDAP Synchronization (version 2)	new
	Oracle DSEE Synchronization (version 2)	new
Domino Module	Lotus Domino synchronization	changed
Exchange Online Module	Exchange Online synchronization (v2)	changed
Privileged Account Governance Module	One Identity Safeguard synchronization	changed
SAP R/3 User Management module Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	changed
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	changed
SAP R/3 Compliance Add-on Module	SAP R/3 authorization objects	changed
SAP R/3 Structural Profiles Add-on Module	SAP R/3 HCM authentication objects	changed
	SAP R/3 HCM employee objects	changed
SharePoint Module	SharePoint synchronization	none
SharePoint Online Module	SharePoint Online synchronization	changed
Universal Cloud Interface Module	SCIM Connect via One Identity Starling Connect	changed
	SCIM synchronization	changed
Unix Based Target Systems Module	Unix Account Management	changed
	AIX Account Management	changed
Target System Synchronization Module	Automatic One Identity Manager synchronization	new

Patches for synchronization projects

Patches for the following patch types are provided in One Identity Manager 8.2.

- Patches for solved issues
- Patches for new functions
- Milestones

To adjust existing synchronization projects to One Identity Manager version 8.2, you must implement milestones. A milestone is provided for each context. A milestone includes all patches for solved issues together with milestones from previous versions, if they have not already been implemented. Once the current milestone has been implemented in a synchronization project, the project is then compatible with One Identity Manager 8.2.

Patches for new functions can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 8.2 for synchronization projects. Only the patches that were newly created after version 8.1.5 are listed. For information about patches from earlier versions of One Identity Manager, see the respective release notes for each version.

Every patch contains a script, which tests whether the patch can be applied to the synchronization project. This depends on the specific configuration of the synchronization.

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

For more information, see Applying patches to synchronization projects on page 88.

Table 15: General patches

Patch ID	Patch	Description	Issue ID
	Milestone 8.2	Milestone for the context **DPR**.	
	Milestone 8.2	Milestone for the context **One Identity Manager**.	

Table 16: 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	Synchronization of `ExternalUserState` and `ExternalUserStateChangeDateTime`	Adds property mapping rules for the `ExternalUserState` and `ExternalUserStateChangeDateTime` schema properties into the `User` mapping.	32665
VPR#32975	Adding a property mapping rule for `LastPasswordChangeDateTime`	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	Milestone for the context **Azure Active Directory**.	

Table 17: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#32110	Adds the `middleName` schema property	Inserts the `middleName` schema property into the	32110

Patch ID	Patch	Description	Issue ID
		User and inetOrgPerson mappings.	
VPR#32759	Adds property mapping rules for the schema property ProtectedFromAccidentalDeletion Deletion	Inserts a property mapping rule for the ProtectedFromAccidentalDeletion schema property 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	Milestone for the context **Active Directory**.	

Table 18: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#32110	New property mapping rule for middleName	Inserts a property mapping rule for the middleName schema property into the User and InetOrgPerson mappings.	32110
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	Milestone for the context **Active Roles**.	

Table 19: 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	Milestone for the context **Oracle E-Business Suite**.	

Table 20: 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	Milestone for the context **Microsoft Exchange**.	

Table 21: 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	Adds a property mapping rule for the `HiddenFromExchange-schema`	34046

Patch ID	Patch	Description	Issue ID
	HiddenFromExchange ClientsEnabled	ClientsEnabled property in the UnifiedGroup mapping.	
	Milestone 8.2	Milestone for the context **Exchange Online**.	

Table 22: 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	Milestone for the context **Google Workspace**.	

Table 23: 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	Milestone for the context **LDAP**.	

Table 24: 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

Patch ID	Patch	Description	Issue ID
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 when One Identity Manager is updated.	34393
	Milestone 8.2	Milestone for the context **HCL Domino**.	

Table 25: 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	Milestone for the context **Privileged Account Management**.	

Table 26: 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

Patch ID	Patch	Description	Issue ID
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 `userInRole` mapping and synchronization step	Corrects the mapping and 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).	34563
	Milestone 8.2	Milestone for the context **SAP R/3**.	

Table 27: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
	Milestone 8.2	Milestone for the context **SAP R/3 structural profile add-on**.	

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

Patch ID	Patch	Description	Issue ID
	Milestone 8.2	Milestone for the context **SAP R/3 analysis authorizations add-on**.	

Table 29: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
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.	32963

Patch ID	Patch	Description	Issue ID
		Part 1: Deletes existing maps. This patch is applied automatically when One Identity Manager is updated. Prerequisite for patch **Mapping changes to map additional 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	Milestone for the context **SAP R/3**.	

Table 30: Patches for SharePoint

Patch ID	Patch	Description	Issue ID
	Milestone 8.2	Milestone for the context **SharePoint**.	

Table 31: 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	Milestone for the context **SharePoint Online**.	

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

Patch ID	Patch	Description	Issue ID
VPR#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 time zone	Adds a variable to the default variable set and connection parameters to be able to set a default time zone. This patch is applied automatically when One Identity Manager is updated.	33978
	Milestone 8.2	Milestone for the context **SCIM**.	

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

Patch ID	Patch	Description	Issue ID
	Milestone 8.2	Milestone for the context **Universal Cloud Interface**.	

Table 34: 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	Milestone for the context **Unix**.	

Table 35: 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	Milestone for the context **Database**.	

Table 36: Patches for the CSV connector

Patch ID	Patch	Description	Issue ID
	Milestone 8.2	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** 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 script 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

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	40 GB

storage	
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 37: Supported data systems

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.
Connector for relational databases	Any relational databases supporting ADO.NET. NOTE: Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer.
Gerneric LDAP connector	Any LDAP directory server conforming to version 3. The LDAP connector requires the directory server to be RFC conform. Specifically, to conform to the standards RFC 4514 (Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names) and RFC 4512 (Lightweight Directory Access Protocol (LDAP): Directory Information Models). NOTE: Other schema and provisioning process adjustments can be made depending on the schema.
Web service connector	Any SOAP web service providing wsdl. NOTE: You can use the web service wizard to generate the configuration to write data to the web service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active	Active Directory shipped with Windows Server 2012, Windows Server

Connector	Supported data systems
Directory connector	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 2010 • SharePoint 2013 • SharePoint 2016 • SharePoint 2019
SAP R/3 connector	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.54, and 7.69 • SAP ECC 5.0 and 6.0 • SAP S/4HANA On-Premise-Edition
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the specifications for One Identity Safeguard Authentication Services.
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
Generic database connector	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe connector	• RACF • IBM i

Connector	Supported data systems
	• CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 7.4.1, 7.4.3, 7.4.4, and 7.4.5
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
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	• One Identity Safeguard version 6.0, 6.7, 6.10, and 6.11

Connector	Supported data systems
Safeguard connector	

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 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 82.

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. 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, different columns that were already semantically defined as mandatory fields become physical mandatory fields.

  During the schema update with the Configuration Wizard, errors may occur due to inconsistent data. The update quits with an error message.

  ```
  <table>.<column> must not be null
  ```

  ```
  Cannot insert the value NULL into column '<column>', table '<table>';
  column does not allow nulls.
  ```

```
UPDATE fails
```

Check and correct data consistency before updating a One Identity Manager database. In the add-on for the Configuration Module on the installation medium, a test script (`\SDK\SQLSamples\Files\MSSQL2K\30374.sql`) is provided. In case it fails, correct the data and restart the update.

- 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 or while updating an One Identity Manager database or One Identity Manager History Database from version 8.0.x to version 8.2, you can specify whether you want to work with granular permissions at server and database level. The Configuration Wizard then creates SQL Server logins and database users with the necessary permissions for administrative user, configuration users and end users. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

  After updating One Identity Manager, change the connection parameters. This affects, for example, the connection data for the database (`DialogDatabase`), the One Identity Manager Service, the application server, the administration and configuration tools, the web applications and web services as well as the connection data in synchronization projects.

> NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 8.2, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.
>
> If you want to switch to granular permissions when you update from 8.1.x, contact support. (missing or bad snippet)

- 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

> IMPORTANT: Note the Advice for updating One Identity Manager on page 82.

To update an existing One Identity Manager installation to version 8.2

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 AZ↓.
   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 program `autorun.exe` from the root directory on the One Identity Manager installation medium.

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

> NOTE:
>
> - To update a One Identity Manager 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, 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. (missing or bad snippet)

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. 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 88.

To update an application server to version 8.2

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

To update the Web Designer Web Portal to version 8.2

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

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

To update an API Server to version 8.2

- After updating the One Identity Manager database schema, restart the API Server. The API Server is updated automatically.

To update the Operations Support Web Portal to version 8.2

- (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. 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 60
- Patches for synchronization projects on page 62

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 2021.0011.0019.0000 for all modules and the application version 8.2 v82-139719 verify that this version is installed.

Additional resources

Additional information is available from the following:

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

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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