One Identity Manager

Release Notes

Version 9.3

13 December 2024, 23:23

These release notes provide information about the One Identity Manager release version 9.3. You will find all the modifications since One Identity Manager version 9.2.1 listed here. For the most recent documents and product information, see Online product documentation.

One Identity Manager 9.3 is a minor release with new functionality and enhanced behavior. See New features on page 2 and Enhancements on page 10.

If you are updating a One Identity Manager version older than One Identity Manager 9.2.1, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under One Identity Manager Support.

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

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

About One Identity Manager

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.

The One Identity Manager enables you to realize Access Governance demands cross-platform within your entire company. One Identity Manager is based on an automation-optimized architecture and, unlike other "traditional" solutions, addresses major identity and access management challenges in a fraction of the time, complexity, and expense.

One Identity Starling

Initiate your subscription within your One Identity on-prem product and join your on-prem solutions to our One Identity Starling cloud platform. Giving your organization immediate access to a number of cloud-delivered microservices, which expand the capabilities of your One Identity on-prem solutions. We will continuously make available new products and features to One Identity Starling.

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

New features

New features in One Identity Manager 9.3:

General

- One Identity Manager is now based on .NET 8.
    - Scripts and all custom extensions must be compatible with .NET 8.
    - NuGet packages are supported as dependencies in scripts.
    - The configuration settings for logging messages using NLog are now made in the `nlog.config` configuration file.
    - General configuration settings for the One Identity Manager tools can be specified in the `appsettings.json` configuration file.

    Due to significant updates, it is not possible to use automatic software to update Job servers and web applications. Therefore, update your Job servers and web applications manually. For more information, see Upgrade and installation instructions on page 61.

    Some functions are no longer supported. For more information, see Deprecated features on page 45.

Custom scripts for synchronization projects that use custom DLL files must be adapted and recompiled. For more information, see Known issues on page 29.

- Automated logging of object changes.

  After objects in One Identity Manager have changed, log messages are automatically generated in CEF (Common Event Format) for a defined subset of changes and sent to a specific syslog server. The types of changes to be logged can be defined in the new QBMCEFDefinitions table, along with message templates and up to five replacement parameters in ObjectWalker notation that relate to the changed object. The connection to the syslog server is configured using the new configuration parameters under **QBM | CEF**.

- The Database Agent Service has been fundamentally revised. The entire process control is now carried out in the Database Agent Service .NET component. The old control procedure QBM_PWorkDBQueueMain, which ran on the database server, is no longer required.

  NOTE: The following tables are read-only views and no longer to be used as a basis for customizations:

    - QBMDBQueueOverview_fix
    - QBMDBQueueOverview
    - QBMDBQueueSlot
    - QBMDBQueueSlot_fix
    - QBMDBQueueTaskPerf
    - QBMDBQueueTaskPerf_fix

- Configuration of DBQueue Processor task processing has been reworked. New configuration parameters:

    - QBM | DBQueue | ChangeLimitDefault
    - QBM | DBQueue | MaxBulkFactor
    - QBM | DBQueue | MaxSlotsPerTask
    - QBM | DBQueue | OverloadLimit

  This change has meant removing configuration parameters. For more information, see Deprecated features on page 45.

- Support of multiple result lists for one menu item.

  The Manager supports the display of more than one result list for a menu item. This makes it easy to switch between multiple result lists. You can specify which columns are displayed in a results list and change the order of the columns. Editing of lists in the Designer has been adapted. An editor is provided for modifying results lists.

  NOTE: Custom menu items are converted during migration. Check these entries after the migration and adjust them further if necessary.

- The new process archive view in Job Queue Info displays completed processes including processes that have already been archived in a History Database. You can apply filters. This view is only shown if a History Database is configured in the

TimeTrace.

- If reports must be displayed in different languages, some characters may not be displayed correctly in all the languages. Use the **Common | UI | ReportAlternateFontname** configuration parameter to define a font that is available on all web servers and clients. Then this font is used to display the reports.

- Email notifications can be sent with Microsoft 365. To do this, an application must be registered in Microsoft Entra ID and declared in One Identity Manager with the new **Common | MailNotification | O365ClientId** configuration parameter.

- Additional data security settings for access via LDAP can be configured for email notifications. New configuration parameters are **Common | MailNotification | Encrypt | AuthenticationType**, **Common | MailNotification | Encrypt | Port**, and **Common | MailNotification | Encrypt | UseSSL**.

- Tables indexing can be configured for full-text search. The new **Common | Indexing | PriorityTables** configuration parameter determines the order in which the search index processes the database tables. The new **Common | Indexing | ExcludeTables** configuration parameter determines which tables are temporarily excluded from indexing.

- Support for loading configuration options for secrets from Azure Key Vault.

- The Manager web application supports logging in via OAuth.

- When creating a transport package with SQL statements in the Database Transporter, single user mode can be enabled or disabled for transport.

- To import transport packages that contain system files with older file versions, users now need the **Common_FileRevisionDowngrade** program function.

- New parameter in the `DBConsCheckCmd.exe` command line program to list and run consistency checks grouped by category.

- New parameter in the `Quantum.MigratorCmd.exe` command line program to force a complete check and repair of the default data during the schema update.

- Installation of a History Database is now also possible without a memory-optimized file group.

- Windows Server 2025 is supported.

API configuration

- The API Server now supports a generic API that accesses tables that have been released for access via the API Server.

- The API Server now enables integration with Microsoft Application Insights. This allows monitoring and analysis of API Server performance. Integration can be carried out with a plugin.

- You can now define your own error messages in API methods that are suited to your use case.

- You can now specify for the Web Portal, whether each request for a system entitlement is checked to see if the recipient has a user account in the target system, and, if necessary, whether to provide a user account for the request. This can be

configured using the **RequestMissingAccounts** configuration key in the Administration Portal.

- In the Administration Portal, it is now possible to use the **AttestationConfig/FilterIdentityApproverInsteadOf** and **ServerConfig/ITShopConfig/FilterIdentityApproverInsteadOf** configuration keys to specify identities that can be delegated request or attestations approvals.

- In the Administration Portal, you can now use the **EnablePasswordProfileLogin** configuration key to configure logging in using password questions.

- In the Administration Portal, it is now possible to use the **ApiConnectionUrl** configuration key to configure the URL of a specific API which clients can use to establish a connection.

- Cross-Origin Resource Sharing (CORS) can now be configured in the Administration Portal using the **CorsOrigins** and **CorsMaxPreflightAgeSeconds** configuration keys.

- In the Administration Portal, you can now configure different Web Portal functions using new configuration keys.

    - EnableWebauthnKeyManagement: Specifies whether users can manage their WebAuthn security keys.

    - EnableNewPerson: Specifies whether users can create identities.

    - ProductSelectionByPeerGroup: Specifies whether products are recommended when putting together a new request by analyzing the recipient's peer group.

    - EnableNewDepartment: Specifies whether users can create departments.

    - EnableNewLocality: Specifies whether users can create locations.

    - EnableNewProfitcenter: Specifies whether users can create cost centers.

    - EnableNewAeRole: Specifies whether users can create application roles for which they are responsible.

    - EnableNewOrg: Specifies whether users can create business roles.

    - EnableNewESet: Specifies whether users can create system roles.

    - EnableNewTeamRole: Specifies whether users can create team roles.

    - EnableNewDelegationSubstitute: Specifies whether users can delegate responsibilities in packages (global delegations).

    - EnableNewDelegationIndividual: Specifies whether users can delegate certain responsibilities separately (individual delegations).

HTML5 web development

- Modified procedure for loading libraries in HTML applications. When compiling an HTML application, care must be taken to ensure that all required libraries are compiled beforehand. This applies regardless of the libraries in which code has been changed.

- The Angular workspace integrates the **Nx** tool for easier dependency management and improved compilation speed.

- In the Web Portal there is now an editor component for properties of type **bitmask**.

HTML5 web applications

- In the Web Portal, you can now share a product with other users so that they can also request the product.

- In the Web Portal it is now possible to display and manage application roles.

- In Web Portal, you can now assign the responsibilities of identities for which you are responsible to other identities.

- An identity administrator can now delegate role memberships and responsibilities of all identities to other identities.

- Some actions that you perform when using Web Portal (for example, approving or denying requests) are processed in the background as so-called background processes. This means you can continue using the Web Portal without interruption. You can now display and manage these background processes.

- In the Operations Support Web Portal, notifications are now displayed on the start page if recommended threshold values from the system report are exceeded.

Target system connection

- Azure Active Direct has been renamed to Microsoft Entra ID.

- The synchronization of user-defined Microsoft Entra ID security attributes is supported.

  A patch with the patch ID ADO#446363 is available for synchronization projects.

- The synchronization of Microsoft Entra ID user accounts sponsors is supported.

  A patch with the patch ID ADO#438166 is available for synchronization projects.

- The synchronization of Microsoft Entra ID temporary access passes is supported in Microsoft Entra ID tenants. Use the configuration parameters under **TargetSystem | AzureAD | Accounts | TemporaryAccessPass** to configure settings for temporary access passes.

  A patch for synchronization projects with the patch ID ADO#446183 is provided.

  NOTE: This function requires **UserAuthenticationMethod.ReadWrite.All** permissions for the One Identity Manager application in Microsoft Entra ID.

- Office 365 has been renamed Microsoft 365.

- Send permissions are now also supported for Exchange Online room mailboxes.

- The Exchange Online connector now uses the `SkipLoadingCmdletHelp` parameter in the `Connect-ExchangeOnline` call, if available. This reduces possible orphaned directories in the temporary folder and eliminates them.

- The creating and editing Microsoft 365 groups (`O3EUnifiedGroup`) via app-only authentication is supported. Subscribers cannot be edited.

  NOTE: This change requires additional permissions **Group.Create**, **Group.ReadWrite.All**, and **GroupMember.ReadWrite.All** for the application registered in Microsoft Entra ID.

- Microsoft Teams channels and teams now have links to the corresponding SharePoint websites.

- Loading of Microsoft Teams channels and teams has been switched to the `/teams` endpoint.

  NOTE: This change requires **TeamSettings.ReadWrite.All** permissions for the One Identity Manager application in Microsoft Entra ID.

- Active Directory, which is supplied with Windows Server 2025, is supported to the same extent as before.

- In order to move user accounts to a special Active Directory container when disabling them, a container for disabled user accounts (`ADSAccount.UID_ADSContainerDisabled`) can be given in the IT operating data.

- After moving a mailbox from a local Microsoft Exchange to Exchange Online, the outstanding mailbox is now automatically deleted.

- Oracle Database 23ai is supported.

- One Identity Safeguard version 8.0 is supported to the previous extent.

- The PowerShell modules for One Identity Safeguard versions 7.0 and 7.5 support .NET 8.

  NOTE: The PowerShell modules must be reinstalled. Copy the directory with the PowerShell module matching the version from the `Modules\PAG\dvd\AddOn\safeguard-ps` directory on the One Identity Manager installation medium to the `%ProgramFiles%\WindowsPowerShell\Modules\safeguard-ps` directory on the server.

- Support for directories as members of PAM asset groups

  A patch with the patch ID ADO#433775 is available for synchronization projects.

- The SDK example and code snippets for retrieving synchronization passwords from One Identity Safeguard for Privileged Passwords have been updated and simplified. For more information, see under `Modules\PAG\dvd\AddOn\SDK`.

- Support for SAP .Net Connector 3.1 for x64 with version 3.1.5 for Microsoft.NET 8.0.x.

- The One Identity Manager Business Application Programming Interface is certified with the SAP S/4HANA Cloud Private Edition, release 2023.

- For more information about the PowerShell connector with detailed instructions and a range of examples, see One Identity GitHub under PowerShell Connector Guide.

Identity and Access Governance

- Use the new **QER | Person | User | DeleteOptions | ReapplyTemplatesOnRestore** configuration parameter to specify whether templates are reapplied when a user account marked for deletion that is managed by account definitions is restored.

- The following subscribable reports have been added.

  - Orphaned user accounts

  - User accounts with above average permissions count

  - Identities with multiple user accounts per target system.

  - Unused user accounts

- The new **PX** - **Identity in any parameter of the request properties** approval procedure enables manual selection of an approver for a request. To do this, a criterion for selecting identities can be stored in a request parameter that the requester uses to select an identity. The selected identity makes the final approval decision for the request. The approval procedure can be used when managers are looking for a deputy, for example. The selected identity becomes the deputy once the request is granted approval.

- Modified definition and calculation of SAP functions. Function arguments can be used to define how the authorization objects are logically linked. The logical operation is saved as a condition for each SAP function.

  - The new **TargetSystem | SAPR3 | SAPRights | AbilityNamePattern** configuration parameter contains the naming convention for the function arguments.

  - The **TargetSystem | SAPR3 | SAPRights | TestWithoutTCD** configuration parameter is no longer required and will be deprecated in future One Identity Manager versions. In version 9.3, the configuration parameter setting can no longer be changed.

  - During the One Identity Manager database update to version 9.3, existing SAP functions are converted to the new procedure.

  - When importing function definitions from older versions of One Identity Manager, these are also converted to the new procedure.

  - There is a new task, **Add via authorization object**, in the permissions editor.

  - It is now possible to enter two different variations of the same authorization object in an authorization definition.

  - Any fields can be added manually in the permissions editor.

  IMPORTANT:

  - Before updating the One Identity Manager database to version 9.3, check the configuration parameter setting.

  - After updating the database and importing function definitions, check the

authorization definitions and the conditions of the converted function definitions before enabling and using the SAP functions.

- If membership is requested or canceled in a system entitlement, the provisioning status of the membership is saved and updated on the request.

- Approval procedures for attestation cases can be divided into stages.

    1. (Optional) Staging

       Those the owners of the respective attestation policy can review the details of an attestation run. If errors are detected the affected attestation cases can be canceled, the errors corrected, and attestation restarted.

    2. Attestation

       Attestation is run according to the defined approval workflow.

    3. (Optional) Challenge

       If an attestation is finally denied, the identities affected can challenge the decision. For example, this prevents entitlements that are needed at short notice from being withdrawn by a scheduled attestation and then having to reassign them again.

    4. (Optional) Automatically withdraw entitlements

       If an attestation is denied in the end, the denied entitlements can be removed immediately.

- Microsoft 365 is now used for attestation by mail. Use the configuration parameters under **QER | Attestation | MailApproval | Mail system** to configure the information required for sending email notifications.

    Microsoft 365 is now used for request approvals by mail. Use the configuration parameters under **QER | ITShop | MailApproval | Mail system** to configure the information required for sending email notifications.

Related topics

Enhancements

The following is a list of enhancements implemented in One Identity Manager 9.3.

Table 1: General

Enhancement	Issue ID
Improved documentation of the `DatabaseAgentServiceCmd.exe` command line program.	427953
Improved how the Configuration Wizard displays warnings and error messages when processing DBQueue Processor tasks.	430668, 36632
Improved documentation for creating database users in the Designer.	430676, 36685
New consistency check **Duplicate Keys in ProxyTable**. This determines whether there are multiple entries in a proxy table that have the same UID, even though the UID should be unique.	431167, 36911
Improved the **Template uses too long columns** consistency check.	432559, 37161
Improved how One Identity Manager tools display date and time in the system journal.	436043
The status page of the application server now shows the connected History Database databases.	439822
Improved behavior of the context menus in Job Queue Info.	441115
Improved behavior when encrypting connection data when restoring a database in the Configuration Wizard.	441175
The `InstallManager.Cli.exe` command line program can now also be run without administrative privileges.	442673
Improved security in Docker images. The port that releases containers has been changed to **8080** for Linux containers and Windows containers. The new **app** user without root permissions is used for Linux containers.	443610
The program settings of the Manager and the Designer have been reworked.	453450
The **SQL Formatter usage test for UID columns** consistency check now provides more precise information about the error location.	453821
Password Manager Secure Password Extension has been updated to version 5.14.2.	454264
Improved process handling to avoid locks in the database if there are a lot of changes being made in parallel.	455268

Enhancement	Issue ID
The name of the authenticated user is now entered in the system journal when login audit is enabled.	456106
Improved Designer-internal full-text search.	456285
Optimized transport of schema extensions using the Database Transporter.	456443, 456397
Optimized initialization of the Designer's internal database. Define the behavior for loading columns in the Designer.	456450
The values of the **Limit** and **Min. time difference [sec]** properties for DBQueue Processor tasks can now be customized.	459207
Improved and more standardized display texts for process tracking.	460026
If the **Common | ProcessState | PropertyLog | AllDefaultPropertiesForModel** configuration parameter is set, the usage (XIsInEffect) and the origin of assignments are now also recorded when changes are made.	460990
When creating tables with the Schema Extension Wizard, the primary key indexes are now created with a row lock.	461386
Improved performance running deferred operations.	462200
The Schema Extension now allows you to remove custom schema extensions for m-to-n and m-to-all tables.	462919
Improved performance of the query filter dialog with large result sets.	463059
Improved performance processing DBQueue Processor tasks that have **1** as the value for the maximum number of instances.	463394
In the Database Compiler, messages for processing the database can be copied to the clipboard with **Ctrl + C**.	467500
Loading reports via an application server does not always take the permissions into account correctly.	468072
Improved performance evaluating the process archive in Job Queue Info.	468290
Only tables that exist in the **dbo** schema are included in automatic index creation.	469029
Missing HTTP response codes have been added in the *One Identity Manager REST API Reference Guide*.	431330

Table 2: API configuration

Enhancement	Issue ID
As the API Server is based on ASP.NET Core, dependencies on Owin have	319906

Enhancement	Issue ID

been removed.

Some APIs have been moved for security reasons.	405504

- The API endpoint **imx/metadata** has been removed. Instead, project-specific endpoints (**portal/metadata** and **opsupport/metadata**) must now be called.
- The **imx/systeminfo/thirdparty** API endpoint has been removed. Instead, project-specific endpoints (**portal/systeminfo/thirdparty**, **opsupport/systeminfo/thirdparty**, and **passwordreset/systeminfo/thirdparty**) must now be called.

The API Server no longer stores the authentication token as a cookie in the browser. All session data is stored in the `QBMSessionStore` table. In addition, persistently stored authentication cookies are no longer supported. All cookies are now only generated as session cookies.	409895

Improved protection against automatic account blocking attacks.	416537

If you use your own API project, you must include the **ProjectLevelConfig** class configuration.

```
var captchaValidator = builder.Resolver.Resolve<ICaptchaValidator>();
var services = builder.Resolver.Resolve<IServices>();
var configService = builder.Resolver.Resolve<IConfigService>();

var projectLevelConfig = new ProjectLevelConfig(captchaValidator);
services.Register(projectLevelConfig);
configService.RegisterConfigurableObject(projectLevelConfig);
```

The application used for configuring Password Reset Portal authentication has been changed to **PasswordReset**. This allows a configuration of authentication modules that only applies to Password Reset Portal.	420909
In the Administration Portal, it is now possible to use the **RecommendationExclude** configuration key to specify which entitlements are not recommended for assignment to objects.	421447
In the Administration Portal, it is now possible to enable or disable logging in to Password Reset Portal with an access code using the **EnablePasscodeLogin** configuration key.	421481
It is now possible to define generic criteria for filtering data using API plugins. A corresponding API example has been provided for this purpose.	440838
It is now possible to add a custom shopping cart check to the Web Portal using a Composition API plugin.	442121

Enhancement	Issue ID
It is now possible to create API methods that support duplicate parameter values.	453412
Improved performance of the request history and certification history in the Web Portal. This change means that the WorkflowSteps property in the API Server response is no longer set individually for each request/attestation case. The previous behavior of the API can be restored by setting the compatibility level with an API plugin as follows.	453959

```
public void Build(IApiBuilder builder) {

            var settings = build-
er.Resolver.Resolve<IMethodSetSettings>();
            settings.CompatibilityLevel =
ApiCompatibilityLevel.Api92;
}
```

Enhancement	Issue ID
The API Server now uses the integrated `System.Text.Json` library instead of the `Newtonsoft.Json` library. General overview: • Property names must now be entered in double quotation marks. • To increase security, special characters are now automatically masked in the JSON code generated by the API Server. The complete list of changes can be found at Migrate from Newtonsoft.Json to System.Text.Json. NOTE: To integrate these changes, you may need to update custom API code.	456940
The Software Development Kit (SDK) with commented code examples for API development can now be found in One IdentityGitHub under Identity Manager API plugin development.	460908

Table 3: HTML5 web development

Enhancement	Issue ID
The source code of the web applications was configured for automatic code formatting with ESLint.	406450
Elemental UI has been updated to Angular version 17/18.	458500
The default value of the content security policy for web applications has been changed to **content-security-policy: object-src 'none'; img-src 'self' data:; default-src: self;**.	460429
Angular has been updated to version 18.2.2.	465211

ONE IDENTITY
by Quest

Table 4: HTML5 web applications

Enhancement	Issue ID
Improved how API documentation is displayed in the Administration Portal.	205843
The Web Portal now displays error messages in a dialog instead of a banner.	268292
If the session expires in a web application, a corresponding message is now displayed and the login page is then loaded.	272514
The Web Portal now supports login with ReCAPTCHA.	284359
Improved attestation of system entitlement owners.	290501
A custom filter condition is now available in the Web Portal to search for products that provide access to a specific entitlement.	312490, 35892
The **Queue** filter has been added to the **Process History** page in the Operations Support Web Portal.	324018
Filters have been added to several pages in the Web Portal: • Attestation History, My Attestations, Pending Attestations: Attestation policy (as default filter) • Attestation Policies, Compliance Rules. and Company Policies: Compliance framework (as custom filter)	324018
When creating new Delayed Logic entities via the API Server, the HTTP status code `201` is now used to show success (used to be `200`).	406394
In web applications, tables can now be sorted by clicking on the column title.	407866
In web applications, you can now simply jump to the first or last page in the tables.	417331
In the Web Portal, an option has been added for policy violations to display only policy violations of a specific object using a custom filter.	426972
The Web Portal now allows elements in hyperviews to be expanded and collapsed.	427822
Improved performance loading large amounts of data in the API Server.	431094
In the Web Portal, it is now possible to carry out actions for multiple requests and attestation cases.	432018
It is now possible to create an empty team role in Web Portal.	432021
The request history in the Web Portal now supports a **My delegations** filter, which filters global and single delegations.	432832

Enhancement	Issue ID
In the Web Portal, the technical names for columns are now also displayed so that it is easier to distinguish between these columns if their display names are the same.	433146
Increased security generating reports.	433758
Improved data display in the Web Portal.	435257
The password questions and answers stored in the Web Portal must now be unique.	435886
The configured display names of the tables and columns are used in the exported SCIM schema and in error messages that refer to specific tables and columns.	436088
Improved how the Web Portal displays an object's history.	437366
The web portal now uses long display names for system entitlements.	441186
In the Web Portal, it is now possible to navigate further in hyperviews based on object properties.	442024
The Web Portal now shows an icon in the header bar that displays the number of products in the shopping cart and goes to the shopping cart.	442136
The Web Portal can now display overviews of objects involved in pending attestation cases as hyperviews.	446465
A message is now displayed in Web Portal if requesting an entitlement for a role leads to a rule violation.	449174
Enhanced performance of the Web Portal home page.	450077
The **DisableHyperViewNavigation** configuration key has been renamed **EnableHyperViewNavigation**.	453647
In the Web Portal, improved performance when displaying user accounts in the Data Explorer.	454162
The Web Portal now correctly recognizes line-wraps as such and displays text correctly.	454683
The RSTS has been updated to version 2024-02-04.1. Changes: • Only image files can still be configured on the RSTS login page. • Support for OAuth2 PKCE and DeviceCode Flow. The RSTS must be uninstalled and reinstalled for the update.	455387
Improved installation of the API Server.	456127
When creating attestation policies in the Web Portal, a message is now	457254

Enhancement	Issue ID
displayed if you have defined a condition that refers to a sample but have not yet selected a sample.	
In the Web Portal, statistics for target systems and namespaces have been added and an option has been created to define KPIs in a hierarchical structure. In addition, the **IHeatmapService** and **IKpiChartService** interfaces have been removed. Only use the **IChartService** interface.	457542
Improved performance in the Web Portal for attestation case approval.	458137
Improved request process for Microsoft Entra ID role assignments and eligibilities.	459668
The Web Portal now also displays a relevant note when displaying attestation cases for properties that have not been set.	460548
The Web Installer normalizes the specified base URL and adds a trailing slash if this is not specified. The base URL of a web application must now be unique.	460949, 460947
Improved usability of the web application login pages.	464184
The search index no longer processes updates of referenced objects. To process changes to referenced objects, start a complete indexing process.	464396
In the Administration Portal it is now possible to configure the HTTP headers that are added to all responses using the **HTTP header** configuration key.	464628
The Web Portal now marks ineffective assignments accordingly for memberships of system entitlements.	464973
Improved support of the API Server for queries with a large number of results from the search index.	465551
When unsuccessful login attempts are logged, the user name used is now abbreviated.	466311
Improved performance for displaying identity responsibilities in the Web Portal.	466408
In the Web Portal, finding optional service items now also takes into account request procedures for multiple identities.	467368

Table 5: Target system connection

Enhancement	Issue ID
Improved mapping of external user IDs for SAP user accounts.	326713
A patch with the patch ID ADO#326713 is available for synchronization	

Enhancement	Issue ID
projects.	
Improved documentation of the synchronization configuration for Exchange Online mailbox permissions.	430716, 36919
Improved documentation of permissions for synchronizing with SharePoint Online.	430723, 37026
The Synchronization Editor now displays a message suggesting that the wizard is used to create new base objects if possible.	430727, 37053
The generic database connector for the generic ADO.NET provider now supports loading from database systems that do not support transactions.	430918, 36210
The schema exported by the Active Directory connector takes into account the `system-only` labeling of attributes in Active Directory and exports these as read-only schema properties. A patch with the patch ID ADO#440672 is available for synchronization projects.	440672
Support for PAM file access requests for accounts in a PAM system. A patch with the patch ID ADO#450685 is available for synchronization projects.	450685
The uniqueness of system entitlement distinguished names in custom target systems has been redefined.	452898
Improved performance running UID comparisons in scripts, templates, and processes.	453649
The restriction on the permitted values for group claims of Microsoft Entra ID app registrations has been removed.	456597
Improved documentation of permissions for registering an application in Microsoft Entra ID.	457262
Most of the SCIM plugin error messages have been standardized for direct database connections and connections via an application server.	458772
The maximum lengths of the `AADGroup.MailNickname` and `AADGroup.DisplayName` columns have been limited according to the lengths in Microsoft Entra ID.	463821
Improved automatic creating of property mapping rules with the Synchronization Editor mapping wizard, which is based on the comparison of similar property names.	438936
The Synchronization Editor Command Line Interface offers additional options to compress the schema and activate the synchronization project after updating a synchronization project.	447064

Enhancement	Issue ID
Synchronization projects can now also be automatically created or updated via a remote connection. The configuration file has been extended to include definitions for establishing the remote connection.	430576
Improved performance processing the **Assign user accounts to SAP parameters** DBQueue Processor task (`SAP-K-UserHasParameter`).	466206
Some Microsoft Entra ID scheme types now support system filters.	439618
Corrected how parameters are passed to functions that are defined in an SAP schema extension file and are used to delete an SAP object.	464030
Optimized creating the central SAP user account for identities. This forms a unique name taking into account all the identity's SAP user accounts. Use the **TargetSystem | SAPR3 | Accounts | CentralSAPAccountGlobalUnique** configuration parameter to define how to format the central SAP user account.	441119

Table 6: Identity and Access Governance

Enhancement	Issue ID
Some statistics have been reworked.	421696
Improved performance when deleting entries from the `Basetree` table.	427842
Improved support for additional properties. • Additional properties and their property groups are now supported in multiple languages. • Additional properties are now visible to every logged-in user. • Additional properties can now be edited in the base data of the individual target systems. The permissions for target system administrators have been reworked.	452775, 452774, 430259, 24441
Improved peer group analysis. Resources that can be requested multiple times are also taken into account.	453951, 433858
The base object of the **VI_Person_Deactive_ExitDate_Expired** scheduled process has been changed to **Identities**.	464512
The reduced risk index for compliance rule copies, company guidelines, and SAP functions is not calculated and no longer displayed in the Manager. The risk index of compliance rules, company guidelines, and SAP functions is only reduced for productive versions by assigning mitigating controls.	469180, 468325
The **AM** - **Manager of the linked identity** approval procedure can now be selected for attesting user accounts in any target system.	459633
Improved performance when notifications are sent about the request or attestation case approvals.	436383

Enhancement	Issue ID
During attestation, terms of use can now be sent as a PDF file. The terms of use can be stored in different languages and are displayed in the respective language of the user.	430379
Random samples can now also be generated as part of sample attestation.	430504
Attestors of service items now see the complete overview form of the respective service item.	430582
A detailed description can now be entered for approval procedures. The description of the default approval procedures contains information about which approvers or attestors are determined and for which requests or base objects of the attestation the approval procedure can be used.	455400
The **Assignment to system role** option in assignment resources is now described in the *One Identity Manager IT Shop Administration Guide*.	458623
Adaptive cards for approving requests or for attestations now also include approval recommendations if this function is configured.	460602
The name and email address of an adaptive cards recipient are updated in the Starling Cloud Assistant if the default email address or the internal name for this identity in One Identity Manager is changed.	456047
Improved performance calculating risk indexes. NOTES: Risk indexes are only calculated on a scheduled basis. Immediate recalculation when data changes no longer take place.	438165, 444303

Related topics

Resolved issues

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

Table 7: General

Resolved issue	Issue ID
An error occurs when transporting schema information (table QBMCustomSQL). Error message: `An item with the same key has already been added`	431395, 37145
The **QER	Person	MasterIdentity	UseMasterForAuthentication**	438952

Resolved issue	Issue ID
configuration parameter is not described correctly in the English One Identity Manager Authorization and Authentication Manual.	
An error occurs when opening any form in a newly installed Manager web application. Error message: `Item has already been added. Key in dictionary: 'XYZ.Forms.dll' Key being added: 'XYZ.Forms.dll'`	439744, 37398
In the Manager web application, filters on assignment forms do not work if the `??` operator is used in the display pattern.	439751
Parameters cannot be edited if an error occurs in the script that determines the value.	441998
The processes history archive also stores process steps that have never been handled.	443585
An error occurs when filling the internal Designer database. Error message: `SQL logic error no such column: XRamState.`	444001
Importing a hotfix transport into a customer database results in a conflict if the same data has been customized.	444145
Under certain conditions, entries in the DBQueue go missing when the Database Agent Service starts and the DBQueue is nearly empty.	445976
Updating the schema can cause the data for `XDateUpDated` and `XUserUpdated` to be set unnecessarily.	446409
Maintaining constraints results in retries not being carried out as intended if an error occurs.	447479
Occasionally, processes that are started by schedules are not created.	453421
Error when running the script for determining the parameter values.	453784
Resource consumption too high and repeated indexing of tables for the search without any changes in the tables.	455394
An error may occur when importing transport packages that contain templates. Error message: `Object was changed by another user.`	455881
Error when running reports via an application server if the report name contains an ampersand (&).	456290
The English `ParameterValue` descriptions of the `ScriptComponent` process component is incorrect.	456662
After installing operating system updates, errors may occur when establishing a connection via the application server	457508

Resolved issue	Issue ID
(`System.Security.Cryptography.CryptographicException`).	
In the process tracking view, processes may not be marked as finished even though processing is complete.	460024
Under certain conditions, process tracking data is generated for a dependent object instead of for the initially changed object.	460068
Logged change actions for tables with a conditional display pattern do not contain a readable display value.	460507
In the Manager, it is necessary to open the main data form in order to see certain tasks.	460569
API servers are not displayed in the Job Queue Info.	460587
Some DBQueue Processor tasks are unnecessarily marked to be run separately.	460633
The column sort order of the data export in Manager does not work correctly for date values.	460847
The SDK example `QBM\dvd\AddOn\SDK\ScriptSamples\07 Expert knowledge\01 External databases.vb` references `VI.DB.Oracle.ViOracleFactory,VI.DB.Oracle`. NOTE: Use the Oracle Data Provider for .NET instead of `VI.DB.Oracle`.	461031
Exporting data to a newly created History Database can result in an error.	461832
When transferring data to the History Database, the **Common | ProcessState | PackageSizeHDB** configuration parameter may not be taken into account.	462986
Archiving process tracking data fails for processes with a large number of dependencies to substituted follow-on processes.	462999
If the minimum password quality for password policies is set to a high value, **4** for example, passwords could not be generated automatically.	463789
Error running the **QBM-K-SetRowLockOnly** DBQueue Processor task if Microsoft Change Data Tracking (CDC) is enabled.	465625
Exporting CSV reports results in the column headings not necessarily being displayed in the correct language of the recipient.	466033
The `QBM_PSetRowLockOnly` procedure does not exclude columnstore indexes from processing.	466200
Defining a filter in Job Queue Info causes an unnecessary confirmation prompt to appear.	466969
Data Import duplicates columns when navigating forward and backward.	467262

Resolved issue	Issue ID
Error inserting custom code snippets in the Script Editor.	469529
Timeout when updating the One Identity Manager database to version 9.2.1 while the QBM_PJobCreate_HOTemplate_B procedure is running.	464312

Table 8: HTML5 web applications

Resolved issue	Issue ID
Identity properties that are blocked from editing can be edited in the Web Portal.	421001
In the Web Portal it is possible to use the dark theme, although it is not supported.	421025
When a session expires an inadequate error message is displayed on the Web Portal login page.	423707
In the Web Portal, devices are incorrectly managed under **Setup > Devices** instead of under **Responsibilities > My responsibilities > Devices**.	424585
In the Web Portal, the shopping cart gave the impression that a partial check or partial submit was possible.	425801
Under certain conditions, selecting requests in the Web Portal can lead to long response times for administrators of organizations and business roles.	431026
On some pages in the Web Portal, the user-defined filters no longer work when grouping data.	433621
No confirmation prompt is displayed when cache is disabled in the Administration Portal.	435111
In the Web Portal, it is possible to generate reports that access tables that the logged-in user is not authorized to read.	437355
In the Web Portal, the search for objects that contribute to a policy violation does not work.	437689
Under certain conditions, automatic removal of memberships during attestation does not work in the Web Portal.	438213
Under certain conditions, requesting SAP authorizations can cause issues in the Web Portal.	438296
The **VI_ITShop_ProductSelectionByReferenceUser** configuration key has no function.	438568
The **ServerConfig/ITShopConfig/VI_ITShop_ ProductSelectionFromTemplate** configuration key has no function.	438570
Scrolling does not work correctly in the Web Portal when creating a new	438778

Resolved issue	Issue ID
report subscription.	
The Web Portal sometimes displays service categories twice on the request page.	439739
In the Web Portal, attestations for a target system that, in the meantime, has been renamed causes an error.	441980
Information is missing in the log view of the Administration Portal.	442530
The number of open sessions is not displayed correctly in the Administration Portal.	442746
Under certain conditions, the Administration Portal does not display the navigation.	444100
In the Web Portal, pending requests data cannot be exported.	444638
In the Web Portal, the sequence of the final result differs from the specified sequence when exporting.	444708
Under certain conditions, an error occurs in the Web Portal when products are displayed.	449292
Performance issues displaying the overview of attestation cases pending approval in the Web Portal.	450286
In the Administration Portal, disabling navigation in hyperviews using the **EnableHyperViewNavigation** configuration key in the API project **Web Portal** also disables navigation in hyperviews in the Operations Support Web Portal.	455119
The Web Portal displays the additional approver as a recipient instead of an additional approver.	455633
In the Web Portal, it is not possible to select dynamic foreign key properties when defining customized filters.	455793
The Web Portal fails to load saved views under certain conditions.	455931
In the Web Portal, it is not possible to approve requests with certain request properties under certain conditions.	456919
In the Web Portal, certain attestation cases cannot be opened via a link.	457344
Requests with a valid-from date in the past cannot be approved in the Web Portal.	457651
The Web Portal does not display the names of some objects correctly in the assignment analysis.	458709
It is not possible to manage disabled reports in the Web Portal.	459392

Resolved issue	Issue ID
In the Web Portal, if provisioning of an application is canceled, all the associated products are incorrectly canceled.	459686
In the Web Portal, it is not possible to search for child service categories on the request page.	459707
In the Web Portal, it is not possible to export pending requests that can be approved by the chief approval team.	460431
In the Web Portal, the delegation process must be restarted if the search for objects to be delegated does not produce any results.	462048
The Web Portal does not display the name of a delegation deputy correctly in the request history.	463587
Under certain conditions, the search for system entitlements or user accounts of specific identities in the Web Portal can produce incomplete results or error messages.	463613
The Web Portal does not export the header when exporting data to CSV.	465136
The Web Portal goes into a request loop if an invalid email address is given in the personal settings.	465213
Under certain conditions, an error occurs in the Web Portal when entitlements are revoked.	465520
The Web Portal does not process requests for API key requests correctly.	465521
Under certain conditions, errors occur in the Web Portal when generating certain reports.	466209
The Web Portal displays details of a request in truncated form in the request history.	466517
Under certain conditions, the Web Portal does not load products on the **New Request** page and an error occurs.	471545
In the Web Portal, requesting products with dependent products does not work under certain conditions.	455814

Table 9: Target system connection

Resolved issue	Issue ID
An error sometimes occurs when removing an account definition.	430573, 36099
In the Designer, under certain conditions, an error occurs when a Job server overview form opens.	430795, 34055
Under certain conditions, `DialogWatchOperation.OperationUser` is not populated correctly.	438921

Resolved issue	Issue ID
An error occurs when configuring auxiliary class assignments for LDAP synchronization projects.	439007
Error in the Exchange Online connector when it converts ISO country codes.	441949
If a quota is reached, no report is created during synchronization simulation.	443647
Under certain conditions, an error occurs when provisioning changes to the country ID of Exchange Online mail users.	452120
No entry is created in the `DPRMemberShipAction` table if pending assignments of administrative units to Microsoft Entra ID user accounts or groups are published in One Identity Manager. Therefore, the assignment is not published.	454690
The `BaseTreeOwnsObject` table is now also used for container objects (`CSMContainer` and `UCIContainer` tables).	455140
During DBQueue Processor task processing, duplicate entries might occur in the `AADScopedRLAsgn` and `AADScopedRLElgb` tables.	457077
An error occurs in the Microsoft Entra ID connection wizard when changing the authentication from delegated entitlements to application entitlements.	457263
In the SCIM plug-in, an incorrect patch request leads to an internal server error.	457486
An error occurs in encrypted databases when loading LDAP connection data in the Synchronization Editor.	457514
An error occurs in the SCIM connector when serializing a PUT request.	457682
In the SCIM plug-in, complex filter expressions for simple attributes and for foreign key relationships cause a list response (ListResponse) and not an error.	458758, 456157
If the **TargetSystem | ADS | ARS_SSM** configuration parameter is set without Active Roles Module being installed, compilation errors occur.	459611

Provisioning of SharePoint Online website collections occasionally fails.
 	
Error message:
 	
`[System.Exception] Unable to resolve site collection.`
 	
`[Microsoft.SharePoint.Client.ServerException] A site already exists at url.`
	463502

Provisioning of SharePoint Online roles or SharePoint Online groups fails if the underlying SharePoint Online website collection was only created shortly beforehand.	465067
A Microsoft Entra ID user account cannot be deleted if there is still a	465287

Resolved issue	Issue ID
SharePoint Online user account dependent on it.	
Loading Microsoft Entra ID user accounts does not work under certain conditions.	468425
Errors that occur when correcting rogue modifications are not included in the synchronization log.	470045
If a custom schema class is used as a member of a virtual schema property with the **Members of M:N schema types** property type, this schema class is sometimes not used during synchronization.	466355
If the authentication type **Ntlm** is disabled, a connection is not established via the RemoteConnectPlugin.	453136
A user account that is marked for deletion in One Identity Manager and has been re-enabled in the target system is not enabled by the synchronization in One Identity Manager.	464211
When editing the schema of a CSV file for an existing system connection in the Synchronization Editor, if a column has the `DateTime` data type selected, the **Timezone** field is not displayed	456049
The **Maps objects referenced by multiple references** option in the Synchronization Editor cannot be enabled on a mapping that has a base mapping assigned to it.	456849
When synchronizing with the One Identity Manager connector, sometimes an object is not imported if an error occurred when synchronizing the previous object.	457199
Target system login using the SCIM connector is not possible if the client secret contains a colon :.	460083
Synchronization sometimes uses more than the permitted 1024 key values for database queries.	462034
Error reading back an object property of a newly created object in a MySQL database. The object is not found in the target system.	462101
Outstanding memberships in system entitlements are converted to a direct membership if they are re-enabled by synchronization.	463620
Performance issues can occur when determining the revision data of One Identity Manager object types.	466991
Error using a remote connection to synchronize a target system. Error message: `Unable to cast object of type 'System.String' to type 'VI.Projector.Data.ISystemObjectData'`	469869
Error applying the patch VPR#37274 to a Microsoft Exchange synchron-	466144

Resolved issue	Issue ID
ization project if an additional variable set exists.	
When provisioning Google Workspace user account properties (such as email addresses, telephone numbers, user details), the `GAP_UserOrganization_Insert/Update/Delete` process sometimes ends with errors.	466239
Error saving Notes user accounts when the spelling (case-sensitive) of first or last names is changed.	469230
The SAP connector does not reliably end the RFC connection between two requests.	459214
The SAP connector does not tolerate incorrect data values.	455745
SAP communication data for identities cannot be saved if no from date is entered.	455667
Error saving changes to the `SAPComSMTP.SMTPAddr` column in the Designer.	432573
When checking an Oracle E-Business Suite schema extension file in the Synchronization Editor, the error message that appears is insufficient.	461818
Provisioning an assignment of a user account to a group in a cloud application is run before the user account is created in the target system.	457459
OAuth authentication for logging in to a cloud application does not work if a combination of application/client ID and additional user name and password is used.	460097
When synchronizing a cloud application via SAP Cloud Identity Services, the PATCH operation does not work for schema properties that are defined in a schema extension.	462827
Error provisioning deleted group memberships if the SCIM provider does not support PATCH operations. Error message: `Internal Server Error`	463886

Table 10: Identity and Access Governance

Resolved issue	Issue ID
An error occurs when saving entries in the `PersonWantsOrg` table with a customized OnSaving script. Error message: `No transaction or savepoint of that name was found.`	433763
Under certain conditions, an error occurs when running DBQueue Processor tasks for the `BaseTreeHasObject` table. Error message: `Violation of PRIMARY KEY constraint 'PK_Basetree_7B2E29F1AC061A4F'. Cannot insert duplicate key in object 'dbo.BasetreeHasObject'.`	454698

Resolved issue	Issue ID
The **AN - Attestor of the system entitlement or system role to attest** approval procedure incorrectly determines product owners instead of attestors of system entitlements. IMPORTANT: The approval procedure has been corrected. Check existing approval workflows that use this procedure. To retain previous functionality, the **AN - Attestor of the system entitlement or system role to attest** approval procedure can be replaced by **EO - Product owner of the system entitlement to attest** in approval steps.	459614
If no country is assigned to an identity, the country entered as the default in the database was not taken into account when determining the fallback.	459962
If responsibility for approving requests or attestations has been delegated, the justification texts from other approval steps are sometimes used in email notifications to the delegators.	465678
If a dynamic role and the associated business role are deleted at the same time, the memberships sometime remain in the system as orphans.	467420
Unnecessary email notification for pending requests if the request has already been automatically assigned.	468164
The **VI_ITShopTempl_UserInterface_and_DisplayRights** permissions group has invalid edit permissions in IT Shop.	469293
The Manager does not sort requests correctly by date in the **Request History** report.	431379
Two additional approval steps are sometimes displayed in the approval history for a product changeover, even though the product was not replaced.	457053
Displaying system entitlements in the Manager on the **Add to IT Shop** form takes a very long time if a large number of objects must be loaded.	458426
Performance issues or errors if a large number of requests are generated almost simultaneously.	458512
Membership in a business role cannot be delegated if the identity became a member of this business role directly and also via a delegation that cannot be delegated on.	459744
In the Manager, request property parameters are not sorted according to the **Sort order** property.	462373
Error requesting a business role assignment.	469739

Related topics

Known issues

The following is a list of issues known to exist at the time of release of this version.

Table 11: General

Known Issue	Issue ID
Error in the Report Editor if columns are used that are defined as keywords in the Report Editor. Workaround: Create the data query as an SQL query and use aliases for the affected columns.	23521
Access errors can occur if several instances of the Web Installer are started at the same time.	24198
Headers in reports saved as CSV do not contain corresponding names.	24657
Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation. Cause: The Configuration Wizard was started directly. Solution: Always use `autorun.exe` for installing One Identity Manager components. This ensures that you do not select any invalid modules.	25315
Error connecting via an application server if the certificate's private key, used by the `VI.DB` to try and encrypt its session data, cannot be exported and the private key is therefore not available to the `VI.DB`. Solution: Mark the private key as exportable if exporting or importing the certificate.	27793
Error resolving events on a view that does not have a UID column as a primary key. Primary keys for objects in One Identity Manager always consist of one, or in the case of M:N tables, two UID columns. This is basic functionality in the system. The definition of a view that uses the `XObjectKey` as primary key, is not permitted and would result in more errors in a lot of other places. The consistency check `Table of type U or R with wrong PK definition` is provided for testing the schema.	29535
If the One Identity Manager database is installed in an SQL cluster (High	30972

Known Issue	Issue ID
Availability Group) and the option DTC_SUPPORT = PER_DB is set, replication between the server is done by Distributed Transaction. If a Save Transaction is run in the process, an error occurs: Cannot use SAVE TRANSACTION within a distributed transaction. Solution: Disable the option DTC_SUPPORT = PER_DB.	
If no date is given, the date 12/30/1899 is used internally. Take this into account when values are compared, for example, when used in reports. For detailed information about displaying dates and time, see the *One Identity Manager Configuration Guide*.	31322
Variables are used in a report and there are customized translations given for these variables in the Report Editor. However, the variables are not translated in the report that is generated. Cause: When reports are generated, the translations of default variables as displayed in the Report Designer dictionary below the **Quest** category are overwritten with the values from the One Identity Manager database. Solution: Create your own variables and store them outside of the **Quest** category in the Report Designer dictionary. These variables can be translated.	36686
The consistency check **Columns of type varchar(38) not PK and not FK.** identifies issues with columns that are varchar(38) long but are not labeled as UID columns. Solution: Choose a different column length when extending the schema. According to the modeling guidelines, columns with a length of varchar(38) are reserved for columns that map a UID.	37072
Installing web applications using the Web Installer in a virtual machine (VM) is not supported if the installation source is located in a shared folder such as a local folder on the VM host that is provided to the VM as a new file drive. The event log may display error messages for **Source = Application error** and **Incorrect application name: WebInstaller.exe**. Workaround: Use a network share and assign it to a free drive letter in your VM.	471381

Table 12: HTML5 web applications

Known Issue	Issue ID
The error message This access control list is not in canonical form and therefore cannot be modified sometimes 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	26739

Known Issue	Issue ID
revoke the changes again.	
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.	32364
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.	
In the Web Portal search, if you enter a search term and then group the data, the view also displays empty groups.	468982

Table 13: Target system connection

Known Issue	Issue ID
Memory leaks occur with PowerShell connections, which use `Import-PSSession` internally.	23795
By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely.	25401
Solution: Make it possible to access the building block **HR_ENTRY_DATE** remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate` in the Synchronization Editor.	
Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses are stored until now.	27042
Error in Domino connector (`Error getting revision of schema type ((Server)))`.	27126
Probable cause: The HCL Domino environment was rebuilt, or numerous entries have been made in the Domino Directory.	
Solution: Update the Domino Directory indexes manually in the HCL Domino environment.	
The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3.	27359
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.	

Known Issue	Issue ID

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 come into effect later. Cause: The `BAPI_EMPLOYEE_GETDATA` function is always run with the current date. Therefore, changes are taken into account on the exact day. Solution: To synchronize personnel data in advance that comes 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

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	32149

type conversion fails.

Solution: Clean up the data.

Workaround: Type conversion can be disabled. For this, SAP .Net Connector for .Net 4.0 on x64, version 3.0.15.0 or later must be installed on the synchronization server.

IMPORTANT: The solution should only be used if there is no alternative because the workaround skips date and time validation entirely.

To disable type conversion

- In the `StdioProcessor.exe.config` file, add the following settings.

    - In the existing `<configSections>`:

      ```
      <sectionGroup name="SAP.Middleware.Connector">

          <section name="GeneralSettings"
          type="SAP.Middleware.Connector.RfcGeneralConfiguratio
          n, sapnco, Version=3.0.0.42, Culture=neutral,
          PublicKeyToken=50436dca5c7f7d23" />

      </sectionGroup>
      ```

    - In the new section:

      ```
      <SAP.Middleware.Connector>

          <GeneralSettings anyDateTimeValueAllowed="true" />

      </SAP.Middleware.Connector>
      ```

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
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
In the schema type definition of a schema extension file for the SAP R/3	33812

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.

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

After upgrading from One Identity Manager version 8.0 or version 8.1 to One Identity Manager version 8.2.1 or later, PowerShell scripts that reference the Az PowerShell module (`Import-Module Az`) may not work. In a PowerShell launched on the same host, the scripts work without errors. Error messages are logged when the `ExecuteScript` process task is run by the `PowerShellComponentNet4` process component.

Issue IDs: 430202, 37116

Example:

`Entry point was not found.`

Cause:

One Identity Manager version 8.2.1 or later, ships with a specific version of an `Azure.Core.dll` library. The custom PowerShell script may however depend on a newer version of the Az PowerShell module. When the One Identity Manager Service runs the script, it uses the locally stored `Azure.Core.dll`, breaking the dependency.

Possible workarounds: Check whether the following workarounds might work with respect to input parameter and return value.

- Call PowerShell as a subprocess

  To run a PowerShell command out of the current process, start a new PowerShell process directly with the command call:

  `pwsh -c 'Invoke-ConflictingCommand'`

- Use the `CommandComponent` process component with the `Execute` process task to launch the PowerShell application with the following command call.

  `powershell -c 'Invoke-ConflictingCommand'`

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**:

Issue IDs: 796028, 30963

`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

Known Issue	Issue ID
displayed as the reason.	
After updating to One Identity Manager version 9.3 or later, scripts in synchronization projects that use custom DLLs can no longer be translated. Cause: Conversion of One Identity Manager base technology to .Net 8. Solution: 1. Transfer these scripts to the Synchronization Editor script library as external scripts. 2. Customize the script code for the use of NuGet packages. 3. Compile the scripts.	463957

Table 14: Identity and Access Governance

Known Issue	Issue ID
During approval of a request with self-service, the `Granted` event of the approval step is not triggered. In custom processes, you can use the `OrderGranted` event instead.	31997
If an assignment is inherited through a role hierarchy, **bit 1** is set on the inherited assignment. Inherited assignments are consequently always indirectly assigned, even if they were originally created directly by a dynamic role or an assignment request.	35193
If a service item has its **Max. days valid** option reduced such that approved requests are already expired, these requests cannot be unsubscribed anymore. Solution: Create a process for the `AccProduct` base object that is triggered when changes are made to `AccProduct.MaxValidDays`. The process calculates the 'valid until' date for these requests (`PersonWantsOrg.ValidUntil`) from `PersonWantsOrg.ValidFrom` and `AccProduct.MaxValidDays`. After which, you can unsubscribe the requests.	36349

Table 15: Third party contributions

Known Issue	Issue ID
Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting **File and Printer sharing** is not set on the server. This option is not set on domain controllers on the grounds of security.	24784
An error, TNS-12516, TNS-12519 or ORA-12520, sporadically occurs when connecting with an Oracle Database. Reconnecting normally solves this.	27830

Known Issue	Issue ID
Possible cause: The number of processes started has reached the limit configured on the server.	
Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages. Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.	29051
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 One Identity does 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 group provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem.	30575
Under certain conditions, the wrong language is used in the Stimulsoft controls in the Report Editor.	31155

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

ONE IDENTITY
by Quest

Schema changes

The following provides an overview of schema changes from version 9.2.1 up to version 9.3.

Configuration Module

- New tables for editing the user interface navigation.
    - `QBMGroupHasTree`
    - `QBMProductHasTree`
    - `QBMTree`
    - `QBMTreeHasColumn`
    - `QBMTreeHasSheet`
    - `QBMTreeHasTreeResult`
    - `QBMTreeHasUIDashBoard`
    - `QBMTreeResult`
    - `QBMTreeResultHasColumn`
    - `QBMTreeResultHasSheet`
    - `QBMUIDashBoard`
- New table `QBMCEFDefinitions` for mapping SIEM messages.
- New table `QBMDBQueueTaskMetric` for processing DBQueue Processor tasks.
- New table `QBMExternalPackage` for mapping external NuGet packages for system compilation.
- New column `DialogColumn.CacheInfo` to specify the behavior when columns are loaded in the Designer.
- New column `DialogColumn.ResultSortOrder` as the default order for displaying the column in result lists or on overview forms.
- New column `DialogDatabase.UID_CutOffTask` for internal use.
- New column `DialogDBQueue.PathLength` to optimize DBQueue Processor processing.
- New column `DialogTable.IsNoProcessMonitoring` to exclude the table from process monitoring.
- New column `QBMClrType.Alias` to group together different implementations of the same interface.
- New column `QBMDBQueueTask.CustomWeight` for customized weighting of the processing sequence for DBQueue Processor tasks.
- New column `QBMFileRevision.SourceType` for optimizing script compilation.
- New column `QBMProduct.UID_QBMTree` as the start menu item for an application.
- The following tables are now read-only views.

- QBMDBQueueOverview_fix
- QBMDBQueueOverview
- QBMDBQueueSlot
- QBMDBQueueSlot_fix
- QBMDBQueueTaskPerf
- QBMDBQueueTaskPerf_fix

- New mandatory field definition for the following columns:
  - DialogMultiLanguage.XObjectKey
  - QBMDBQueueTask.XObjectKey
  - QBMDBQueueTaskDepend.XObjectKey
  - QBMFileRevision.XObjectKey
  - QBMMissingDisplayRight.XObjectKey
  - QBMModuleDef.XObjectKey
  - QBMModuleDepend.XObjectKey
  - QBMNonLinearDepend.XObjectKey
  - QBMRelation.XObjectKey
  - QBMXUser.XObjectKey

- The DialogDatabase.CustomerName column has been extended to nvarchar(256).
- The DialogHistoryDB.TransportConnectionString column has been extended to varchar(max).
- The data type of the DialogSheet.SortOrder column has been changed to nvarchar(7).
- The following tables have been deleted.
  - DialogAEDSAction
  - DialogAEDSActionHasObject
  - DialogAEDSActionType
  - DialogGroupHasTree
  - DialogTree
  - DialogTreeHasSheet
  - DialogTreeInDialogProduct
  - QBMDBQueueSlot
  - QBMDBQueueTaskDependCollection
  - QBMDevBranch
  - QBMDevBranchHasAssembly

- The following tables have been deleted.

- DialogColumn.BitMaskConfig
- DialogColumn.LimitedValues
- DialogDBQueue.SortOrder
- QBMDBQueueCurrent.SortOrder
- QBMDBQueuePond.noCheckForExisting
- QBMDBQueuePond.SortOrder
- QBMDBQueueSlot.CountToLoad
- QBMDBQueueSlot.RunningState
- QBMDBQueueSlot.ServerProcess
- QBMDBQueueSlot.SlotNumber
- QBMDBQueueSlot.UID_QBMDBQueueSlot
- QBMDBQueueSlot.UID_Task
- QBMDBQueueSlot.XObjectKey
- QBMDBQueueTask.CountSingleSteps
- QBMDBQueueTask.IsUnusedInSimulation
- QBMDBQueueTask.LastExecutedAt
- QBMDBQueueTask.MaxBulk
- QBMDBQueueTask.MinBulk
- QBMDBQueueTask.SingleTime
- QBMDBQueueTask.SortOrder
- QBMProduct.UID_DialogTree
- QBMWebApplication.UID_DialogAEDSWebProject
- QBMWebApplication.UID_DialogAuthentifier
- QBMWebApplication.UID_DialogAuthSecondary

Target System Synchronization Module

- New column DPRScript.IsExternal for scripts with external references to NuGet packages.
- New mandatory field definition for the DPRScript.UID_DPRShell and DPRScript.UID_QBMClrType columns.

Target System Base Module

- New mandatory field definition for the TSBITData.XObjectKey and TSBITDataMapping.XObjectKey columns.

Microsoft Entra ID Module

- New tables to support Microsoft Entra ID security attributes.
    - `AADSecAttrDef`
    - `AADSecAttrSet`
    - `AADSecAttrSvcPInstance`
    - `AADSecAttrUsrInstance`
- New table `AADUserSponsor` for mapping sponsors of Microsoft Entra ID user accounts.
- New table `AADUserTemporaryAccessPass` for mapping temporary access passes for Microsoft Entra ID user accounts.
- New column `AADOrganization.SyncTags` for mapping additional synchronization data.
- New column `AADUser.XDateSubItem` for mapping the change date of dependent objects.

Exchange Online Module

- New mandatory field definition for the `O3EMailbox.XObjectKey` column.
- The `O3EMailbox.AdditionalResponse` column has been extended to `nvarchar(max)`.
- The `O3EUnifiedGroup.SharePointDocumentsUrl`, `O3EUnifiedGroup.SharePointNotebookUrl`, and `O3EUnifiedGroup.SharePointSiteUrl` columns have been extended to `nvarchar(max)`.

Microsoft Teams Module

- New column `O3TTeamChannel.ObjectKeyO3SSite` for linking a SharePoint website.

Active Directory Module

- New column `ADSAccount.UID_ADSContainerDisabled` as container for disabled Active Directory user accounts.

Microsoft Exchange Module

- New mandatory field definition for the following columns:
    - `EX0DL.XObjectKey`
    - `EX0DynDL.XObjectKey`
    - `EX0MailBox.XObjectKey`
    - `EX0Server.XObjectKey`

Privileged Account Governance Module

- New columns to support access requests for files:
  - `PAGAstAccount.AllowFileRequest`
  - `PAGAstAccount.HasFile`
  - `PAGDirAccount.AllowFileRequest`
  - `PAGDirAccount.HasFile`
  - `PAGUserAttestation.AllowFileRequest`
- New columns `PAGAssetInAstGroup.ObjectKeyMember` and `PAGAssetInAstGroup.UID_PAGAssetInAstGroup` for mapping group memberships.
- The `PAGAssetInAstGroup.UID_PAGAsset` column has been deleted.

SAP R/3 User Management Module

- The `SAPComSMTP.SMTPAddr` column has been shortened to `nvarchar(241)`.

Identity Management Base Module

- New table `QERRiskIndexColumnDepend` for defining dependencies between risk indexes.
- New column `PWODecisionRule.Remarks` for a better description of the approval procedures.
- New columns for the use of samples in attestation.
  - `QERPickCategory.CreateRandomSampleForEachRun`
  - `QERPickCategory.IsRandomSample`
  - `QERPickCategory.RandomSamplePickRate`
  - `QERPickCategory.RandomSampleWhereClause`
- The `PersonPasswordHistory` table has been deleted.
- The `QERRiskIndexHasSourceTable` table has been deleted.
- The `PWODecisionRule.IsSimulationBased` column has been deleted.
- The `QERRiskIndex.IsExecuteImmediate` column has been deleted.

Attestation Module

- New column `AttestationObject.UiChallengeText` queries when challenging attestation approvals.

SAP R/3 Compliance Add-on Module

- New tables and new columns to support SAP functions and calculations.
    - SACAbility
    - SACAbilityFI
    - SACFunctionInstanceHasAO
    - SACFunctionInstHasAbilityFI
    - SACProfileHasAbilityFI
    - SAPFunction ConditionString
    - SAPFunctionDetail.UID_SACAbility
    - SAPFunctionInstanceDetail.UID_SACAbility
    - SAPFunctionInstanceDetail.UID_SACAbilityFI
- The SAPFunctionDetail.LowerLimit and SAPFunctionInstanceDetail.LowerLimit columns have been extended to nvarchar(max).
- New mandatory field definition for the SAPRCTable.XObjectKey column.
- The SAPProfileHasTCDinFID table has been deleted.
- The following tables have been deleted.
    - SAPFunctionDetail.AUTHOBJNAM
    - SAPFunctionDetail.AUTHOBJTYP
    - SAPFunctionDetail.AUTHPGMID
    - SAPFunctionDetail.RFC_NAME
    - SAPFunctionDetail.RFC_TYPE
    - SAPFunctionDetail.SAPHashValue
    - SAPFunctionDetail.SRV_NAME
    - SAPFunctionDetail.SRV_TYPE
    - SAPFunctionDetail.TCD
    - SAPFunctionDetail.UID_SACTransactionType
    - SAPFunctionInstanceDetail.UID_SAPTransaction

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 9.2.1 up to version 9.3. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 64.

New and deleted synchronization templates

No new synchronization templates are provided in One Identity Manager 9.3. No synchronization templates were deleted.

Patches are provided for changes to existing synchronization templates. For more information, see Patches for synchronization projects on page 43.

Patches for synchronization projects

Patches for the following patch types are provided in One Identity Manager 9.3.

- Patches for resolved issues
- Patches for new features
- Milestones

To adjust existing synchronization projects to One Identity Manager version 9.3, you must implement milestones. A milestone is provided for each context. A milestone includes all patches for resolved issues together with milestones from previous versions if they have not already been implemented. Once the current milestone has been implemented in a synchronization project, the project is then compatible with One Identity Manager 9.3.

Patches for new features can be applied optionally.

The following is a list of all new patches provided in One Identity Manager 9.3 for synchronization projects. Only the patches that were newly created after version 9.2.1 are listed. For information about patches from earlier versions of One Identity Manager, see the respective release notes for each version.

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

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

For more information, see Applying patches to synchronization projects on page 64.

Table 16: Patches for Microsoft Entra ID

Patch ID	Patch	Description	Issue ID
ADO#446363	Support for Microsoft Entra ID security attributes	Extends the synchronization configuration to support Microsoft Entra ID security attributes on user accounts and service principals. This patch is applied automatically when One Identity Manager is updated.	446363
ADO#438166	New property	Inserts a new property mapping rule in	438166

Patch ID	Patch	Description	Issue ID
	mapping rules for mapping sponsors for user accounts	the `User` mapping for mapping sponsors for user accounts. This patch is applied automatically when One Identity Manager is updated.	
ADO#446183	Support for Microsoft Entra ID temporary access passes	Extends the synchronization configuration to support Microsoft Entra ID temporary access passes for user accounts in Microsoft Entra ID tenants. This patch is applied automatically when One Identity Manager is updated.	446183

Table 17: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
ADO#440672	Marks system schema properties as `read-only`	Updates the target system schema to mark schema properties as read-only if they are marked as `System-Only` in Active Directory. This patch is applied automatically when One Identity Manager is updated.	440672

Table 18: Patches for Privileged Account Management

Patch ID	Patch	Description	Issue ID
VPR#37283	Support for directories as members of PAM asset groups	Extends the synchronization configuration to support directories as members of PAM asset groups. This patch is applied automatically when One Identity Manager is updated.	433775
ADO#450685	Support for One Identity Safeguard 7.5	Extends the synchronization configuration to support One Identity Safeguard version 7.5.	450685

Table 19: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
ADO#326713	Corrects the `userExternalID` mapping	Corrects the mapping for external identifiers. Removes the `vrtExtID_EXTID` property mapping rule.	326713

Table 20: Patches for SharePoint

Patch ID	Patch	Description	Issue ID
ADO#419381	Support for ports in connection parameters	Extends the connection parameters by specifying the port for the SharePoint connector to communicate internally. This patch is applied automatically when One Identity Manager is updated.	440892

Deprecated features

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

- The following features are no longer supported in the One Identity Manager Service.
    - FileJobProvider
    - FileJobDestination
    - FileJobGate
    - FTPJobProvider
    - FTPJobDestination
    - HTTPJobProvider
    - HTTPJobDestination
    - HTTPJobGate
- The Web Designer and Web Designer-based web applications are no longer supported. Use the HTML web applications that are provided via the API Server.
- When the Manager is in simulation mode, processing of DBQueue Processor tasks, such as recalculating compliance rules, is no longer supported. This affects the **Identity Audit Simulation** and **Identity Audit Simulation Evaluation** plugins as well as the **VID_DatabaseSimulationResult_with_Compliance_Export** report.
- The SQL Server 2019 version for the One Identity Manager database is no longer supported.
- Synchronization with Microsoft Exchange 2013 is no longer supported.
- Synchronization with SharePoint 2013 is no longer supported.

- The use of classic authentication using user name and password to synchronize with SharePoint Online is no longer supported. SharePoint Online synchronization projects must be converted to certificate-based login.

- One Identity Active Roles versions 7.x are no longer supported.

- One Identity Safeguard versions 6.x, 7.1, 7.2, 7.3, and 7.4 are no longer supported.

- The `PowerShellComponent` process component is no longer supported. Use the `PowershellComponentNet4` process component instead.

- Container support for Windows Server 2016 will be discontinued.

- Web Service Wizard for integrating SOAP or WCF web services has been removed. SOAP web services are disabled during migration as they are no longer supported. Documentation is provided on integrating web services via NuGet packages.

- Due to the new program structure, it is no longer possible to pre-compile assemblies in the Designer and then transfer them to the database. The **Process > Compile and save to database** menu item has been removed from the Process Editor.

- The `globallog.config` configuration file is no longer supported.

- The **ServerConfig/ITShopConfig/VI_ITShop_Employee_Preselected** configuration key for the Web Portal has been removed.

- The **CaptchaCaseInsensitive** and **CaptchaTestKey** configuration keys have been removed for the **API Server**, **Web application overview**, and **scim** API projects.

- In the Administration Portal, various configuration keys under **ServiceCatalogViewConfiguration** have been removed.

- The following scripts were deleted.

    - VI_AE_BuildCentralAccount

    - VI_AE_BuildCentralAccountGlobalUnique

    - VI_BuildInternalName

    - VI_AE_CreatedefaultMailAddress

    - VI_AE_BuildCentralSAPAccount

  NOTE: The script was used in earlier versions of One Identity Manager in templates for the `Person` table. Check the templates and any other customized usage of these scripts.

- The following scripts were deleted.

    - QER_CloudAssistant_LifeCycle

    - VI_MailApproval_ProcessInBox

    - VI_MailApproval_ProcessMail

    - VID_GetWebService

- The following configuration parameters are not used in the Database Agent Service anymore and have been removed.

- QBM | DBServerAgent

- QBM | DBServerAgent| CountSlotAgents

- QBM | DBServerAgent | CreateNotification

- QBM | DBQueue | ChangeLimitMax

- QBM | DBQueue | ChangeLimitMin

- The **TargetSystem | SAPR3 | SAPRights | TestWithoutTCD** configuration parameter can no longer be modified. To change the processing logic of SAP functions, use the logical expression that is stored in each function definition. The logical expression for existing function definitions from versions older than 9.3 is calculated taking the configuration parameter into account. For more information, see Enhancements on page 10. (Issue ID 438883)

- Running process functions externally as a separate 32-bit process is no longer supported. The process functions have been deleted.

  NOTE: Customized uses of process functions are adapted during migration. Check your processes after migration.

- Connecting CData ADO.NET Provider databases with the generic database connector is no longer supported.

- Risk indexes are no longer recalculated immediately when data changes. They are only calculated on a scheduled basis.

The following features will be deprecated in future releases of One Identity Manager and should no longer be used:

- Support for Windows Server 2012 and Windows Server 2012 R2 will be deprecated in future releases.

- The **TargetSystem | SAPR3 | SAPRights | TestWithoutTCD** configuration parameter will be deprecated in future versions.

System requirements

Before installing One Identity Manager 9.3, ensure that your system meets the following minimum hardware and software requirements.

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. For more information about environment virtualization, see One Identity's Product Support Policies.

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.

Supported database systems

One Identity Manager supports the following database systems:

- SQL Server
- Managed instances in the Azure SQL Database
- Azure SQL Database
- Amazon RDS for SQL Server

Minimum system requirements for implementing SQL Servers as database servers

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.

Table 21: Minimum system requirements for SQL Servers

Requirement	Detail
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

Requirement	Detail
	• Note the minimum requirements given by the operating system manufacturer for SQL Server databases.
Software	Following versions are supported: • SQL Server 2022 Standard Edition (64-bit) with the latest cumulative update NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems. NOTE: Ledger is not supported. For more information, see the Knowledge Base. • Compatibility level for databases: SQL Server 2022 (160) • Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) • SQL Server Management Studio (recommended)

NOTE: The minimum requirements listed above are 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 environment virtualization, see One Identity's Product Support Policies.

Requirements for a managed instance in Azure SQL Database

For more information about Azure SQL Database, refer to the Microsoft website under https://azure.microsoft.com/en-us/products/azure-sql/database/.

The following requirements and limitations apply to the use of a managed instance in Azure SQL Database as a database system.

- The **Business Critical** tier is required.
- Ledger is not supported. For more information, see the Knowledge Base.

Requirements for Azure SQL Database as database system

For more information about Azure SQL Database, refer to the Microsoft website under https://azure.microsoft.com/en-us/products/azure-sql/database/.

The following requirements and limitations apply to the use of Azure SQL Database as a database system.

- If you use Azure SQL Database as the database system, you must supply a database. There is no support for creating a new database in Azure SQL Database with the Configuration Wizard.
- use statements are not supported.
- Strong passwords must be used for the SQL login.

  For more information, see under Strong Passwords in the Microsoft documentation.
- Ledger is not supported. For more information, see the Knowledge Base.

Requirements for Amazon RDS for SQL Server as database system

The following requirements and limitations apply to the use of Amazon RDS for SQL Server as a database system.

- If you use Amazon RDS for SQL Server as the database system, you must supply a database. There is no support for creating a new database in Amazon RDS for SQL Server with the Configuration Wizard.
- The granular permissions concept is not supported.

Minimum requirements for administrative workstations

A minimum of the following system prerequisites must be fulfilled before installing the One Identity Manager components on an administrative workstation.

Table 22: Minimum system requirements for administrative workstations

Requirement	Detail
Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	5 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
Additional software	• .NET 8.0 SDK with the current service pack • Microsoft Edge WebView2
Supported browsers	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimum requirements for Job servers

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

Table 23: Minimum system requirements for Job servers

Requirement	Detail
Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems The following versions are supported:

Requirement	Detail
	• Windows Server 2025
	• Windows Server 2022
	• Windows Server 2019
	• Windows Server 2016
	• Windows Server 2012 R2
	• Windows Server 2012
	Linux operating systems
	• Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems
	• .NET 8 Desktop Runtime
	NOTE: Take the target system manufacturer's recommendations for connecting the target system into account.
	Linux operating systems
	• .NET 8 Runtime
	NOTE: It is recommended to use .Net container images.

Minimum requirements for API Servers

A minimum of the following system prerequisites must be fulfilled to install an API Server.

Table 24: Minimum system requirements for API Servers

Requirement	Detail
Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems
	The following versions are supported:
	• Windows Server 2025
	• Windows Server 2022
	• Windows Server 2019

Requirement	Detail
	• Windows Server 2016
	• Windows Server 2012 R2
	• Windows Server 2012
	Linux operating systems
	• Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems
	• ASP.NET Core Windows Hosting Bundle
	• Microsoft Internet Information Services 10 or 8.5, or 8 with the role services:
	• Web Server > Common HTTP Features > Static Content
	• Web Server > Common HTTP Features > Default Document
	• 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
	• ASP.NET Core Runtime
	NOTE: It is recommended to use .Net container images.
	• ASP.NET Core Hosting process manager, deployed via Docker container

Minimum requirements for application servers

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

Table 25: Minimum system requirements for application servers

Requirement	Detail
Processor	8 physical cores 2.5 GHz+
Memory	8 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems The following versions are supported: • Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Docker images for Linux distributions supported by the .NET project

Additional software	Windows operating systems
	
	• ASP.NET Core Windows Hosting Bundle
	• Microsoft Internet Information Services 10 or 8.5, or 8 with the role services:
	
	    • Web Server > Common HTTP Features > Static Content
	    • Web Server > Common HTTP Features > Default Document
	    • Web Server > Application Development > ISAPI Extensions
	    • Web Server > Application Development > ISAPI Filters
	    • Web Server > Security > Basic Authentication
	    • Web Server > Security > Windows Authentication

Requirement	Detail
	• Web Server > Performance > Static Content Compression
	• Web Server > Performance > Dynamic Content Compression

Linux operating system

- ASP.NET Core Runtime

  | NOTE: It is recommended to use .Net container images.

- ASP.NET Core Hosting process manager, deployed via Docker container

Supported data systems

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

Table 26: 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.
Generic 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.
Active Directory connector	Active Directory shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019,Windows Server 2022, and Windows Server 2025.
Microsoft Exchange connector	• Microsoft Exchange 2016

Connector	Supported data systems
	• Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange Hybrid environments
SharePoint connector	• SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
SAP R/3 connector	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55, 7.56, 7.57, 7.58, and 7.69 • SAP ECC 5.0 and 6.0 • SAP S/4HANA On-Premise Edition 1.0 and 2.0 as from SAP BASIS 7.40 SR 2 and 7.50 (also for installing with SAP BASIS 7.53) • SAP S/4HANA Cloud 2022 and 2023 with SAP BASIS 7.57 and 7.58 • SAP .Net Connector 3.1 for x64, with at least version 3.1.5 for Microsoft .NET 8.0.x
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the specifications for One Identity Authentication Services.
Domino connector	• HCL Domino Server versions 12 and 14 • HCL Notes Client versions 12.0.1 (only 64 bit) and 14.0 The same major version is used for the HCL Domino Server and the HCL Notes Client.
Generic database connector	• SQL Server • Oracle Database • SQLite • MySQL • DB2 (LUW) • SAP HANA • PostgreSQL
Mainframe connector	• RACF • IBM i • CA Top Secret

Connector	Supported data systems
	• CA ACF2
PowerShell connector	• PowerShell Version 7.x or later
Active Roles connector	• One Identity Active Roles 8.0, 8.1.1, 8.1.3, and 8.1.5

Microsoft Entra ID connector	• Microsoft Entra ID
	
	NOTE: Synchronization of Microsoft Entra ID tenants in national cloud deployments with the Microsoft Entra ID connector is not supported.
	
	This affects:
	
	   • Microsoft Cloud for US Government (L5)
	   • Microsoft Cloud Germany
	   • Microsoft Entra ID 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 version 12.1, 12.2, 12.2.10, 12.2.11, 12.2.12, and 12.2.13
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard version 7.0, 7.5, and 8.0 You can find the PowerShell module to match each supported version in the `Modules\PAG\dvd\AddOn\safeguard-ps` directory on the One Identity Manager installation medium. Versions without a matching PowerShell module on the One Identity Manager installation medium are not supported.

Long Term Support (LTS) and Feature Releases

You can choose between two paths for receiving releases: Long Term Support (LTS) Release or Feature Release.

Long Term Support (LTS)

- The initial One Identity Manager LTS release is 9.0. For all LTS releases of One Identity Manager, the first digit identifies the release and the second is always a zero (for example, 9.0).
- Maintenance LTS Releases (known as Cumulative Updates): A third digit is added; for example, 9.0.1.

Feature Release

- Feature Releases' version numbers are two digits (for example, 9.1, 9.2, 9.3 etc).

The table below shows a comparison of Long Term Support (LTS) Release and Feature Release.

Table 27: Comparison of Long Term Support (LTS) Release and Feature Release

Category	Long Term Support (LTS) Release	Feature Release
Release frequency	Every 36 months (includes resolved issues and security related updates).	Approximately every 12 months (includes resolved issues and security related updates).
Duration of full support	36 months	18 months
Duration of limited support	12 months (after the end of full support)	6 months (after the end of full support)
Versioning	All versions where the second number is **0**. For example: 9.0.0 (9.0.1, 9.0.2,), 10.0.0, 11.0.0, and so on.	All versions where the second number is not **0**. For example: 9.1.0 (9.1.1, 9.1.2), 9.2, 9.3, and so on.
Duration of service pack availability between releases	Approximately every 6 months, cumulative updates (CUs) are expected for each LTS release.	Every 6 months patch releases (service pack) are expected for each feature release currently supported.
Criteria for issuing hotfixes for LTS outside of a cumulative update	• The product is not functioning after installing the most recent CU and the customer cannot wait until the next CU	

Category	Long Term Support (LTS) Release	Feature Release
cycle	is available. • The product is not functioning/is inoperable which is causing a production outage/serious issue. • A security related fix is needed on a priority basis to address a vulnerability. • No fixes will be issued to implement an enhancement outside of the cumulative update cycle.	

Release details can be found at Product Life Cycle.

One Identity strongly recommends always installing the latest revision of the release path chosen by the customers/partners (Long Term Support path or Feature Release path).

Moving between LTS versions and Feature Release versions

You can move from an LTS version (for example, 9.0 LTS) by installing a later feature release or version (for example 9.3). Once this has happened, you are not on the LTS support path until the next LTS base version (10.0, etc.) is installed.

You can move from a Feature Release to an LTS Release, but only to an LTS release with a later version. For example, you cannot move from 9.3 to 9.0 LTS. You have to keep upgrading with each new Feature Release until the next LTS Release version is published. For this example, you would wait until 10.0 LTS is available.

Patches

For LTS, there are no patches released, only hotfixes, and these are distributed only in rare cases. Refer to the previous table to see the criteria for LTS hotfixes. These hotfixes need to be applied in order of their release.

LTS has periodic cumulative updates (CUs) provided for LTS customers, which roll out the issues resolved during that period. It is not required to install every CU separately. For instance, if CU1 is released followed by CU 2, you do not need to install CU1 before installing CU2. The CUs are cumulative.

For more information, see the knowledge article 4372133.

For customers on the feature release option track, maintenance releases are cumulative, meaning that maintenance releases do not need intermediate releases to be installed to update to a newer maintenance release. This is unchanged from previous versions. For example, if you want currently use version 9.1.1 and want to upgrade to 9.3, and, for example, versions 9.1.3, 9.1.4, and 9.1.5 have been released, you only have to install version 9.3 and it automatically applies the resolved issues from 9.1.3, 9.1.4, and 9.1.5.

Frequently Asked Questions (FAQs)

What is Long Term Support (LTS)?

- LTS is a support option that allows you to stay on the same release for an extended period of time while still receiving the high level of support that One Identity is known for. While on the LTS path, you receive updates aimed at resolving issues and vulnerabilities. There are not, however, any product enhancements or features delivered while on the LTS release.

What are the benefits to being on an LTS release?

- Some enterprises have a difficult time in keeping up with the migration to new releases in a timely manner to fit within the vendor's support guidelines. This allows the enterprise to stay on one version for a considerable amount of time.

What are the disadvantages to being on an LTS release?

- The negatives, of course, are missing out on receiving the latest enhancements and features from the vendor.

Duration of an LTS release

- A Long Term Support (LTS) version provides you with up to 3 years of support after the original release date or until the next LTS release (which ever date is later); with an option to continue via Extended Security Support (ESS).

How do I make the move to the LTS support option?

- When you install an LTS version, such as One Identity Manager 9.0, you are automatically on the LTS path. The choice you make for the next release that you install, determines whether you remain on LTS or go to the traditional support model.

Once I choose to go on the LTS path, can I ever move back to the feature release path?

- Yes. You can do this by installing a later maintenance version or feature release. For example, if you currently have version 9.0 (LTS) and decide to move to 9.3, you will come off the LTS support path until you install the next base LTS version (10.0, etc.)

Is there an extra charge if I choose the LTS option?

- No, long term support is included in your annual maintenance renewal. An option to continue limited support is offered at an additional charge via our Extended Security Support (ESS).

Product licensing

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

Upgrade and installation instructions

To install One Identity Manager 9.3 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

Take note of the following information when updating One Identity Manager.

- One Identity Manager version 9.3 does not support the Data Governance Edition. If you want to update a database on which the Data Governance module is installed, you must uninstall this module before you can perform the update. For more information about how to remove modules, see the One Identity Manager Installation Guide.

- Evaluate changes in a test system before you load a migration package into a production system. Use a copy of the production database for testing.

- Ensure that the administrative system user, who is going to compile the database, has a password before you update the One Identity Manager database to version 9.3. 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 to version 9.3, different columns that were already semantically defined as mandatory fields become physical mandatory fields.

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

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

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

  UPDATE fails
  ```

  Check and correct data consistency before updating a One Identity Manager database. In the add-on for the Configuration Module on the installation medium, a test script (`\SDK\SQLSamples\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 accesses. 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.

- 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*.

- Use the `Modules\QBM\dvd\AddOn\SDK\SQLSamples\MSSQL2K\SDK_Remove_Rights_on_msdb.sql` SDK script to remove permissions that are no longer required for the msdb database.

- It is not recommended to perform an upgrade of the existing modules to a new One Identity Manager version and install additional modules at the same time. This may cause dependencies between modules to be constructed incorrectly. First update the existing modules to the new One Identity Manager version. Then restart the Configuration Wizard and install the additional modules.

Updating One Identity Manager to version 9.3

IMPORTANT: Note the Advice for updating One Identity Manager on page 61.

IMPORTANT: One Identity Manager version 9.3 does not support Data Governance Edition. If you want to update a database on which the Data Governance module is installed, you must uninstall this module before you can perform the update. For more information about how to remove modules, see the One Identity Manager Installation Guide.

NOTE: This One Identity Manager version contains significant updates that do not allow the use of automatic software updates for Job servers and web applications. Therefore, update your Job servers and web applications manually.

To update an existing One Identity Manager installation to version 9.3

1. End and uninstall the web applications.

2. Stop the One Identity Manager Service on all Job servers.

3. Run all the consistency checks in the Designer in **Database** section.

   a. In the Designer, start the Consistency Editor with the **Database > Check data consistency** menu item.

   b. In the **Test options** dialog, click 🔽.

   c. Under the **Database** node, enable all the tests and click **OK**.

   d. Start testing with the **Consistency check > Run** menu item.

      All the database tests must be successful. Correct any errors. Some consistency checks offer repair options for correcting errors.

4. Update the administrative workstation, on which the One Identity Manager database schema update is started.

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

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

   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.

5. Make a backup of the One Identity Manager database.

6. Update the One Identity Manager database. 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.

7. Reinstall the web applications.

8. Update all program and service components on all Job servers. Use the installation wizard.

9. Start the One Identity Manager Service on all Job servers.

10. Update the other workstations. You can use the automatic software update method for updating existing installations.

To update synchronization projects to version 9.3

1. If you have set up synchronization projects for connecting cloud applications in the Universal Cloud Interface, update the target system schema in these synchronization projects using the Synchronization Editor.

2. Any required changes to system connectors or the synchronization engine are made available when you update One Identity Manager. These changes must be applied to existing synchronization projects to prevent target system synchronizations that are already set up, from failing. Patches are made available for this.

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

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

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

Applying patches to synchronization projects

⚠ **CAUTION: Patches do not alter custom changes in synchronization projects. This means that conflicts may occur if patches are applied to synchronization projects that have been customized. It may cause loss of data.**

Before you apply a patch

1. Read the patch description to decide whether it provides the necessary improvements for the synchronization project.

2. Check whether conflicts with customizations could occur.

3. Create a backup of the database so that you can restore the original state if necessary.

4. (Optional) Deactivate the synchronization project.

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

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

To apply patches

1. In the Synchronization Editor, open the synchronization project.

2. Select the **Edit > Update synchronization project** menu item.

3. In **Available patches**, select the patches you want to apply. Multi-select is possible.

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

4. Click **Apply selected patches**.

5. Enter any user input as prompted.

6. Use the patch log to check whether customization need to be reworked.

7. If required, rework customizations in the synchronization configuration.

8. Run a consistency check.

9. Simulate the synchronization.

10. (Optional) Activate the synchronization project.

11. Save the changes.

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

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

See also:

- New and deleted synchronization templates on page 43
- Patches for synchronization projects on page 43

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 2024.0011.0030.0000 for all modules and the application version 9.3 v93-278876 indicate that this version is installed.

Additional resources

More information is available under:

- 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