One Identity Manager 9.1.3

Release Notes

25 April 2024, 12:32

These release notes provide information about the One Identity Manager release version 9.1.3. You will find all the modifications since One Identity Manager version 9.1.2 listed here.
For the most recent documents and product information, see Online product documentation.

One Identity Manager 9.1.3 is a patch release with new functionality and improved behavior. See New features on page 2 and Enhancements on page 3.

If you are updating a One Identity Manager version older than One Identity Manager 9.1.2, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under One Identity Manager Support.

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

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

About One Identity Manager 9.1.3

One Identity Manager simplifies the process of managing user identities, access permissions, and security policies. It gives control over identity management and access decisions to your organization, freeing up the IT team to focus on their core competence.

With this product, you can:

- Implement group management using self-service and attestation for Active Directory with the One Identity Manager Active Directory Edition
- Realize Access Governance demands cross-platform within your entire company with One Identity Manager

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

One Identity Starling

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

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

New features

New features in One Identity Manager 9.1.3:

Target system connection

- One Identity Safeguard version 7.5 is supported to the previous extent.

Identity and Access Governance

- Support for new **Manual laborer** employee type. The employee type is included in the license report for One Identity Manager.

See also:

- Enhancements on page 3
- Resolved issues on page 4

- Schema changes on page 19
- Patches for synchronization projects on page 22

Enhancements

The following is a list of enhancements implemented in One Identity Manager 9.1.3.

Table 1: General

Enhancement	Issue ID
Third-party component Oracle.ManagedDataAccess updated.	439029, 37394
Enhanced documentation of the **No direct database connection** property for Job servers.	440489, 37435
Enhanced performance when creating and handling processes.	443099
Enhanced re-creation of index for the `DialogDBQueue` table.	443120
Enhanced documentation of the wizard for entering database queries.	445717
Enhanced performance of Job server querying the Job queue.	445982
Configuration parameters can now be marked as encrypted even if database encryption is not configured.	446349

Table 2: HTML5 web applications

Enhancement	Issue ID
Enhanced performance loading products on the request page in the Web Portal.	431052, 36716
Enhanced performance of the Web Portal home page.	431110, 36837
If OAuth is not configured correctly, more meaningful error messages are now generated for the API Server log.	437362
In the Administration Portal, you can now define a filter using the **VI_ITShop_Filter_AccProduct** configuration key. This filter determines which service items are displayed in the Web Portal depending on the selected request recipients.	445150
In the Administration Portal, you can now define a filter using the **VI_ITShop_Filter_AccProductGroup** configuration key. This filter determines which service categories are displayed in the Web Portal depending on the selected request recipients.	445150

Table 3: Web Designer web applications

Enhancement	Issue ID
Enhanced performance when copying items in the Web Designer Web Portal shopping cart.	446254
Performance submitting the shopping cart in the Web Designer Web Portal has been enhanced, when the **VI_ITShop_CalculateComplianceCheck** configuration key is disabled.	449152

Table 4: Target system connection

Enhancement	Issue ID
The generic database connector for PostgreSQL databases supports the `Name` and `OID` data types.	447959

Table 5: Identity and Access Governance

Enhancement	Issue ID
Functional changes in the SAP R/3 Compliance Add-on (SAC) module have been rolled back to a stable version.	447665

See also:

- Schema changes on page 19
- Patches for synchronization projects on page 22

Resolved issues

The following is a list of issues addressed in this release.

Table 6: General

Resolved issue	Issue ID
An update migration from One Identity Manager versions 8.1.x or 8.2.x with granulated permissions to versions 9.0, 9.1, or 9.2 leaves behind permissions for the msdb database that are no longer required. NOTE: 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.	430965, 36480
Using single sign-on to log in to the Manager does not work if the web application is connected via an application server.	431124, 36849

Resolved issue	Issue ID
Token authentication on the application server using OAuth2.0/OpenID Connect on the `/api/script/...` endpoint does not work.	431256, 37025
An error occurs logging in to the Launchpad via OAuth.	436327, 37289
Errors can occur when process history records are transferred to the History Database. Error message: `Cannot insert duplicate key in object 'dbo.HistoryJob'.`	438926, 37336
An error sometimes occurs when a session is discarded in the application server client. Error message: `System.ObjectDisposedException: The session is already disposed.`	438971, 37367
If the SQL Server name contains special character (such `\`, `?`, or `:`), the Database Transporter generates an invalid name for the transport file. Special character are replaced with an underscore (_).	439766
In certain constellations, schedules are started twice within a minute.	440501, 37439
Incorrect calculation and evaluation in reports depending on whether historical assignments are in effect or not.	440795
An error occurs transporting change labels that contain delete operations on schema data. Error message: `Object of type Additional view definition does not exist in database or you do not have the relevant viewing permissions.`	441417
After reactivating process steps, warnings are recorded in the system journal.	441496
Clicking elements in the result list sometimes triggers a drag and drop event that might result in subsequent errors.	441687
The DBQueue Processor task for creating database server permissions fails if the schema name contains a backslash (\).	441824
If the **Address** parameter in a process that sends an email notification is empty, the process does not fail.	442110
If a failed process step is manually forwarded to the error branch or the success branch, the information is logged in the subsequent process step.	442773
If the top process step in a process is moved, the necessity to compile is not detected.	443440

Resolved issue	Issue ID
Performance issues running the maintenance task to reduce the process history.	445873
Under certain conditions, deleting entries from the system journal causes performance problems or blocks the database.	447189
Under certain conditions, an error occurs when running the **SQL Clause Executable (QER)** consistency check.	448312
The English country code for the Republic of Türkiye has been corrected (Türkiye).	448328
Performance issues after updating a History Database.	449127

Table 7: HTML5 web applications

Resolved issue	Issue ID
In the Web Portal, the search sometimes stops and displays an error.	298020
The list of approvers and attestors in the Web Portal is not complete.	418493
When a manager selects their employees' compliance violations, the queries can take a long time.	430675, 36684
In the Web Portal, an error occurs when checking the shopping cart if the requested product has a request parameter that contains a list of permitted values.	431120, 36847
In the Web Portal, request properties for products in a service category are not inherited correctly by the products in the child service categories.	431218, 36991
Under certain conditions, the search for devices does not work in the Web Portal.	436349, 37299
The Web Portal does not update the number of pending requests, attestations, and rule violations.	439550, 446476
In the Web Portal, it is possible to create a delegation although the mandatory field **Valid until** is empty.	439722, 37364
The Web Portal does not transfer all the request parameters for products to the shopping cart.	440206, 37386
In the Operations Support Web Portal, process steps that are not at root level cannot be run again.	442934
In the Web Portal, an error occurs if you open the shopping cart containing a product that is not assigned to a service category.	444242
Under certain conditions, it is not possible to login to the Password Reset Portal with a passcode.	444749
In the Web Portal, an error occurs if a pending attestation case is opened.	450403

Table 8: Web Designer web applications

Resolved issue	Issue ID
Under certain conditions, you cannot display logs in the Web Designer Monitor.	431165, 36910
In the Web Designer, it is possible to select the **Extended properties** options on a **Warning** node.	431199
Hyperviews of system entitlements cannot be displayed in the Web Designer Web Portal.	438977, 37369
The Web Designer Web Portal incorrectly displays a time picker for the **Disable until** property in identity main data.	440431
In the Web Designer Web Portal, editing properties of multiple products in the shopping cart does not work properly.	440970
Editing or deleting view settings in the Web Designer Web Portal causes an error.	442097
In the Web Designer Web Portal, pressing the **Enter** key in the filter dialog does not always work.	442101
The Web Designer Web Portal does not correctly identify all time zones. This causes an error.	442109

Table 9: Target system connection

Resolved issue	Issue ID
Error provisioning outstanding cloud user accounts.	430832, 35201
When testing the connection settings in the project wizard, the SCIM connector cannot establish a connection to the cloud application if OAuth authentication is used and the connection parameter contains special characters.	433792, 37260
An error sometimes sporadically occurs when evaluating a synchronization simulation. Error message: `Object not set to a reference of an object.`	436301, 37279
An error occurs loading LDAP groups with a lot of members. Error message: `Invalid data. Data of type (System.Object[]) is not supported.`	438967, 37365
Error loading a PostgreSQL database schema. Error message: `[System.OverflowException] Arithmetic operation resulted in an overflow.`	438984, 37371
After changing the membership in a system entitlement, the DBQueue Processor task for updating the `XDateSubItem` column is not reset, even	438992, 37376

Resolved issue	Issue ID
though there are processing tasks for the same object in the Job queue.	
Group memberships of Azure Active Directory user accounts are deleted when the corresponding memberships in Exchange Online are enabled.	439006, 37384
When synchronizing SAP authorization objects, not all objects in the `USOBHASH` table are read into the One Identity Manager database if SAP BASIS version 7.57 (SAP S/4HANA 2022) or later is in use in the synchronized SAP R/3 environment. Import the current `SAPTRANSPORT_70.ZIP` transport into the SAP R/3 system you want to synchronize. This uses the `/VIAENET/LISTUSOBHASH` function module instead of the `AUTH_TRACE_GET_USOBHASH` SAP module. When accessing SAP R/3, the SAP R/3 connector checks whether the `/VIAENET/LISTUSOBHASH` function module is available and uses it. This synchronizes all objects in the `USOBHASH` table. The synchronization log records whether the `/VIAENET/LISTUSOBHASH` function module is used.	440164
Some of the PAM asset group and PAM account group columns are too short.	440493, 37437
Error writing data to tables in a PostgreSQL database if the table contains a column whose value is incremented automatically.	440899
Under certain conditions, an error occurs when synchronizing Exchange Online. Error message: `You must call Connect-ExchangeOnline before calling any other cmdlet.`	440909
A system user who has read-only permissions can still delete, reset, and publish objects on the form for target system synchronization objects.	441968
Error requesting a cloud group if a cloud permissions control is assigned to this group.	442501
Error setting up synchronization with the generic database connector for the generic ADO.NET provider, SAP HANA databases, and DB2 (LUW) databases if the connection configuration is loaded from a UDL file. Error message: `DistributionConnector: Error connecting the system. Unable to load the UDL file.`	442883
If several synchronizations are run in parallel from a start up sequence and at least two synchronizations are completed at the same time, it is possible that the start up sequence never completes.	443582
Error connecting to a cloud application using the SCIM connector if authenticating via the OAuth protocol 2.0. A patch with the patch ID ADO#444262 is available for synchronization projects.	444262

Resolved issue	Issue ID
In the Manager, an account definition cannot be selected on the main data form when creating a new Active Directory contact.	444696
Target system objects that are loaded in the One Identity Manager database via a remote connection sometimes have incorrect display names.	446392
Some steps are missing in the report on simulating a synchronization with revision filtering.	446827
One Identity Safeguard users who use Active Directory as their identity provider cannot be removed from local One Identity Safeguard user groups.	447214
Occasionally, when re-enabling a failed process for creating Active Directory user accounts, a user account might be created without a password although the password was originally set.	448865
The Exchange Online mailbox permissions for full access are not synchronized correctly.	449217

Table 10: Identity and Access Governance

Resolved issue	Issue ID
Performance issues deleting an IT Shop shelf.	436343, 37296
Under certain conditions, email notifications about a request approval are not sent, even though email notifications are configured correctly.	438917, 37328
If a product is canceled while the request renewal process is running, the renewal workflow is run instead of the cancellation workflow.	438935, 37344
For the XM, CM, and PW approval procedures, attestors are not recalculated if an attestor has delegated the approval.	438946, 37354
Performance issues loading the list of attestation cases.	438951, 444125, 37356
The `SAC_FTProfileInSAPFunction` function returns incorrect results if an SAP function consists of more than one transaction. This leads to unexpected results, depending on the order of the transactions within the SAP function.	439016, 37389
Incorrect recalculation of the attestors if a regular attestor is initially also a member of the chief approval team and is later removed from this group.	439757, 37407
Sometimes IT Shop requests are canceled if a shelf is moved to another shop, even though the **Retain service item assignment on relocation** option is enabled on the service item.	441274
If an approval step is escalated, the request is automatically canceled under the following conditions (and not submitted to the escalation approvers):	441330

Resolved issue	Issue ID
- An approver from the next escalation approval step escalates the request manually. - The **QER | ITShop | AutoDecision** configuration parameter is set.	
The product owners of system roles, subscribable reports, and software cannot see the overview forms of the responsible product.	442050
Occasional performance problems when processing the DBQueue Processor `QER-K-PWOHelperFillMakeProc` task.	443432
Performance issues when determining the manager permissions for the `Person` table.	446706

See also:

- Schema changes on page 19
- Patches for synchronization projects on page 22

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

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	27793

Known Issue	Issue ID
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.	
Error resolving events on a view that does not have a UID column as a primary key. Primary keys for objects in One Identity Manager always consist of one, or in the case of M:N tables, two UID columns. This is basic functionality in the system. The definition of a view that uses the `XObjectKey` as primary key, is not permitted and would result in more errors in a lot of other places. The consistency check **Table of type U or R with wrong PK definition** is provided for testing the schema.	29535
If the One Identity Manager database is installed in an SQL cluster (High Availability Group) and the option `DTC_SUPPORT = PER_DB` is set, replication between the server is done by Distributed Transaction. If a `Save Transaction` is run in the process, an error occurs: `Cannot use SAVE TRANSACTION within a distributed transaction`. Solution: Disable the option `DTC_SUPPORT = PER_DB`.	30972
If no date is given, the date 12/30/1899 is used internally. Take this into account when values are compared, for example, when used in reports. For detailed information about displaying dates and time, see the *One Identity Manager Configuration Guide*.	31322
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

Table 12: 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 revoke the changes again.	26739
In the Web Portal, a product’s request properties are not transferred from the original request to the shopping cart if the request is renewed or canceled. Cause: Request properties are saved in separate custom columns. Solution: Create a template for (custom) columns in the `ShoppingCartItem` table that stores the request properties when the request is made. This template must load the request properties from the identical (custom) columns in the `PersonWantsOrg` table relating to this request.	32364
It is not possible to use the Web Designer to place a link in the header of the Web Portal next to the company name/logo.	32830
In the Web Portal, it is possible to subscribe to a report without selecting a schedule. Workaround: • Create an extension to the respective form, which displays a text message under the menu explaining the problem. • Add a default schedule to the subscribable report. • In the Web Designer, change the **Filter for subscribable reports** configuration key (**VI_Reporting_Subscription_Filter-RPSSubscription**) and set the schedule's **Minimum character count** value (`UID_DialogSchedule`) to **1**.	32938

If the application is supplemented with custom DLL files, an incorrect version of the `Newtonsoft.Json.dll` file might be loaded. This can cause the following error when running the application:
`System.InvalidOperationException: Method may only be called on a Type for which Type.IsGenericParameter is true.`
`at System.RuntimeType.get_DeclaringMethod()`
There are two possible solutions to the problem:
• The custom DLLs are compiled against the same version of the `Newtonsoft.Json.dll` to resolve the version conflict.
• Define a rerouting of the assembly in the corresponding configuration
	33867

Known Issue	Issue ID

file (for example, `web.config`).
Example:
`<assemblyBinding >`
`<dependentAssembly>`
`<assemblyIdentity name="Newtonsoft.Json"`
`publicKeyToken="30AD4FE6B2A6AEED" culture="neutral"/>`
`<bindingRedirect oldVersion="0.0.0.0-11.0.0.0"`
`newVersion="11.0.0.0"/>`
`</dependentAssembly>`
`</assemblyBinding>`	

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

Table 13: Target system connection

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

Known Issue	Issue ID
• Add a custom column to the table `SAPUser`. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required.	
Error provisioning licenses in a central user administration's child system. Message: `No company is assigned`. Cause: No company name could be found for the user account. Solution: Ensure that either: • A company, which exists in the central system, is assigned to user account. - OR - • A company is assigned to the central system.	29253
Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will 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
The following error occurs in One Identity Safeguard if you request access to an asset from the access request policy section and it is configured for asset-based session access of type **User Supplied**: `400: Bad Request -- 60639: A valid account must be identified in the request.` The request is denied in One Identity Manager and the error in the request is displayed as the reason.	796028, 30963
Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled. Cause: The SharePoint connector loads all object properties into cache by default. Solution: • Correct the error in the target system.	31017

<table>
<tr><th>Known Issue</th><th>Issue ID</th></tr>
<tr><td>

- OR -

- Disable the cache in the file `VI.Projector.SharePoint.<Version>.Host.exe.config`.

</td><td></td></tr>
<tr><td>

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.

</td><td>31904</td></tr>
<tr><td>

If date fields in an SAP R/3 environment contain values that are not in a valid date or time formats, the SAP connector cannot read these values because type conversion fails.

Solution: Clean up the data.

Workaround: Type conversion can be disabled. For this, SAP .Net Connector for .Net 4.8 on x64, version 3.1.2.0 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=3.1.2.42, Culture=neutral,
         PublicKeyToken=50436dca5c7f7d23" />

    </sectionGroup>
    ```

  - In the new section:

    ```
    <SAP.Middleware.Connector>

         <GeneralSettings anyDateTimeValueAllowed="true" />

    </SAP.Middleware.Connector>
    ```

</td><td>32149</td></tr>
<tr><td>

There are no error messages in the file that is generated in the `PowershellComponentNet4` process component, in `OutputFile` parameter.

Cause:

No messages are collected in the file (parameter `OutputFile`). The file serves as an export file for objects returned in the pipeline.

</td><td>32945</td></tr>
</table>

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

Known Issue	Issue ID

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.
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'`
	37116

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	36349

Known Issue	Issue ID
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.	
In One Identity Manager 9.1.3 or older versions, rule conditions cannot be read by compliance rules that were created with One Identity Manager 9.2 or newer.	35131

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. Possible cause: The number of processes started has reached the limit configured on the server.	27830
Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages. Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.	29051
Valid CSS code causes an error under Mono if duplicate keys are used. For more information, see https://github.com/mono/mono/issues/7455.	762534, 762548, 29607
Memberships in Active Directory groups of type **Universal** in a subdomain are not removed from the target system if one of the following Windows updates is installed: • Windows Server 2016: KB4462928 • Windows Server 2012 R2: KB4462926, KB4462921 • Windows Server 2008 R2: KB4462926 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

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

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

Schema changes

The following provides an overview of schema changes from version 9.1.2 up to version 9.1.3.

Privileged Account Governance Module

- The columns `PAGAstGroup.AssetGroupingRule`, `PAGAccGroup.DirectoryAccountGroupingRule`, and `PAGAccGroup.AssetAccountGroupingRule` have been extended to `nvarchar(max)`.

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 9.1.2 up to version 9.1.3. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 52.

Modified synchronization templates

The following provides you with an overview of synchronization templates. Patches are made available for updating synchronization templates in existing synchronization projects. For more information, see Patches for synchronization projects on page 22.

Table 16: Overview of synchronization templates and patches

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

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

Patches for synchronization projects

The following is a list of all patches provided for synchronization projects in One Identity Manager 9.1.3. Every patch contains a script, which tests whether the patch can be applied to the synchronization project. This depends on the specific configuration of the synchronization.

For more information, see Applying patches to synchronization projects on page 52.

Table 17: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
ADO#444262	New variable for configuring the transfer of access data	Inserts the `dprauthoauthusebody` variable into the standard variable set and the connection parameters. This can be used to configure the transfer of access data in the header or body. This patch is applied automatically when One Identity Manager is updated.	444262

Patches in One Identity Manager version 9.1.2

Table 18: General patches

Patch ID	Patch	Description	Issue ID
VPR#36755	Disables the synchronization buffer for the central database	Disables the synchronization buffer for various virtual schema properties in the central database schema in synchronization projects for system synchronization.	36755

Table 19: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#36799	Sets filters in multi-reference rules	Inserts member filters in various multi-reference rules for the `Owners` schema property. This patch is applied automatically when One Identity Manager is updated.	36799

Table 20: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#37274	Adjusts variable descriptions	Adjusts descriptions of variables for synchronization projects. This patch is applied automatically when One Identity Manager is updated.	37274

Table 21: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#36970	Sets reload threshold of user accounts	Sets the reload threshold in the user synchronization step to the value **4**.	36970

Table 22: Patches for SharePoint Online

Patch ID	Patch	Description	Issue ID
VPR#37272	Set filters for the vrtLcid and vrtLanguage schema properties	Sets system filters in the vrtLcid and vrtLanguage schema properties in the Site, Web, and WebTemplate mappings.	37272

Table 23: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#36985	Schema extension corrections	Saves the name of the schema type extensions in the schema. This patch is applied automatically when One Identity Manager is updated.	36985

Patches in One Identity Manager Version 9.1.1

Table 24: Patches for Active Directory

Patch ID	Patch	Description	Issue ID
VPR#35808	Correction of the property mapping rule for StructuralObjectClass	Corrects the StructuralObjectClass_vrtobjectClass property mapping rule in the domainDNS mapping. **Ignore case** is enabled. This patch is applied automatically when One Identity Manager is updated.	35808

Table 25: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#36151	Correction of property mapping rules for Mailbox database and	Corrects the property mapping rule for Mailbox database and Archive mailbox database in the Mailbox mapping, to prevent changes to mailbox databases in One Identity Manager being overwritten	36151

Patch ID	Patch	Description	Issue ID
	Archive mailbox database	by old values. This patch is applied automatically when One Identity Manager is updated.	

Table 26: Patches for LDAP

Patch ID	Patch	Description	Issue ID
VPR#36271	New property mapping rule for the UserPassword schema property	Inserts a property mapping rule for the UserPassword schema property into the User and InetOrgPerson mappings.	36271
VPR#36450	New property mapping rule for the AccountDisabled schema property	Inserts a property mapping rule for the AccountDisabled schema property into all mappings with the LDAPAccount schema type.	36450

Table 27: Patches for HCL Domino

Patch ID	Patch	Description	Issue ID
VPR#35816	Correction of the InternetAddress mapping	Corrects details of the vrtInternetAddress1st schema property in the Database, Group, and Person mappings. This patch is applied automatically when One Identity Manager is updated.	35816

Table 28: Patches for OneLogin

Patch ID	Patch	Description	Issue ID
VPR#35969	Correction of schema properties for resolving references	Corrects details of schema properties from the OLGEvent (all) schema class. This patch is applied automatically when One Identity Manager is updated.	35969

Table 29: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#35991	Correction of property mapping	Sets the **Force mapping against direction of synchronization** option	35991

Patch ID	Patch	Description	Issue ID
	rules in the userExternalID mapping	on various property mapping rules in the userExternalID mapping. This patch is applied automatically when One Identity Manager is updated.	

Table 30: Patches for SAP R/3 authorization objects

Patch ID	Patch	Description	Issue ID
VPR#35944	Correction of the reload threshold in the start up configuration	Increases the reload threshold in the **Initial Synchronization** start up configuration. This patch is applied automatically when One Identity Manager is updated.	35944

Table 31: Patches for the SCIM interface (in Universal Cloud Interface Module)

Patch ID	Patch	Description	Issue ID
VPR#36108	Updates the target system schema	Updates the target system schema. This patch is applied automatically when One Identity Manager is updated.	36108

Table 32: Patches for the Universal Cloud Interface (in Cloud Systems Management Module)

Patch ID	Patch	Description	Issue ID
VPR#36150	Correction of handling ineffective assignments in the Provisioning workflow	Extends a condition on the Insert processing method in synchronization steps for handling memberships of cloud groups and cloud system entitlements in the Provisioning workflow. This prevents provisioning of ineffective assignments.	36150

Patches in One Identity Manager version 9.1

Table 33: General patches

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

Table 34: Patches for Azure Active Directory

Patch ID	Patch	Description	Issue ID
VPR#33400	New property mapping rule for assigning administrator roles to Azure Active Directory groups	Adds a property mapping rule for the `IsAssignableToRole` schema property to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated. Dependent on the **Filter members of directory roles** patch (VPR#33399).	33400
VPR#34744	New property mapping rule for mapping the properties of dynamic Azure Active Directory groups	Adds property mapping rules for the `membershipRuleProcessingState` and `membershipRule` schema properties to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated.	34744
VPR#35033	Support for B2C tenants	Adds property mapping rules for the `TenantType` and `Identities` schema properties in the `Organization` and `User` mappings.	35033
VPR#35286	Allows writing of email addresses of Azure Active Directory user accounts.	Corrects the property mapping rule for the `Mail` schema property in the `User` mapping. This patch is applied automatically when One Identity Manager is updated.	35286
VPR#35289	Support for administrative units	Extends the synchronization configuration to support administrative units. This patch is applied automatically when One Identity Manager is updated.	35289
VPR#35290	New property mapping rule for the creation type of Azure Active Directory user accounts.	Adds a property mapping rule for the `CreationType` schema property to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated.	35290

Patch ID	Patch	Description	Issue ID
VPR#35303_ AAD	Supports classifications	Extends the synchronization configuration to support classification of Exchange Online Office 365 groups.	35303
VPR#35768	Correction of the `ServicePrincipal` mapping	Corrects the property mapping rule for the `Owners` schema property in the `ServicePrincipal` mapping. This patch is applied automatically when One Identity Manager is updated. Depending on patch **Azure Active Directory service principal support** (VPR#33088).	35768
	Milestone 9.1	Milestone for the context **Azure Active Directory**.	

Table 35: Patches for Active Directory

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

Table 36: Patches for Active Roles

Patch ID	Patch	Description	Issue ID
VPR#35122	Updates the target system schema	Updates the target system schema to update data types in the stored schema.	35122

Patch ID	Patch	Description	Issue ID
		This patch is applied automatically when One Identity Manager is updated.	
	Milestone 9.1	Milestone for the context **Active Roles**.	

Table 37: Patches for Microsoft Exchange

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

Table 38: Patches for Exchange Online

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

Patch ID	Patch	Description	Issue ID
	ficate-based authentication	the default variable set. This patch is applied automatically when One Identity Manager is updated.	
VPR#35343_O3E	Supports classifications	Extends the synchronization configuration to support classification of Exchange Online Office 365 groups. This patch is applied automatically when One Identity Manager is updated.	35303
	Milestone 9.1	Milestone for the context **Exchange Online**.	

Table 39: Patches for Microsoft Teams

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

Table 40: Patches for Google Workspace

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

Table 41: Patches for LDAP

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

Table 42: Patches for HCL Domino

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

Table 43: Patches for OneLogin

Patch ID	Patch	Description	Issue ID
VPR#35834	New object matching rule in the `UserCustomAttribute` mapping	Inserts another object matching rule in the `UserCustomAttribute` mapping. This patch is applied automatically when One Identity Manager is updated.	35834

Table 44: Patches for Privileged Account Management

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

Table 45: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#34646_SAP	Updates the target system	Updates the target system schema.	34646

Patch ID	Patch	Description	Issue ID
	schema	This patch is applied automatically when One Identity Manager is updated.	
	Milestone 9.1	Milestone for the context **SAP R/3**.	

Table 46: Patches for SAP R/3 personnel planning data and structural profiles

Patch ID	Patch	Description	Issue ID
VPR#32154	Introduces some revision counters	Enables revision filtering in the **Main Identity**, **Workdates of Employee**, and **Communication Data** synchronization steps.	32154
	Milestone 9.1	Milestone for the context **SAP R/3 structural profile add-on**.	

Table 47: Patches for SAP R/3 BI analysis authorizations

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

Table 48: Patches for SAP R/3 authorization objects

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

Table 49: Patches for SharePoint

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

Table 50: Patches for SharePoint Online

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

Table 51: Patches for the SCIM interface (in Universal Cloud Interface Module)

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

Table 52: Patches for the Universal Cloud Interface (in Cloud Systems Management Module)

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

Table 53: Patches for Unix

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

Table 54: Patches for the One Identity Manager connector

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

Table 55: Patches for the CSV connector

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

Deprecated features

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

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

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

  Added instructions in the One Identity Manager API Development Guide on how to convert XML-based API definition code into a plugin library.
- Administration of different versions of a compiled project using compilation branches is no longer supported.
- The Visual Studio Code extension for HTML application development is no longer supported.
- Compiling HTML applications in the Database Compiler is no longer supported.
- The SharePoint 2010 connector is no longer supported.
- The Microsoft Exchange 2010 connector is no longer supported.
- The **Relevance for compliance** property for IT Shop requests (`PWODecisionStep.ComplianceRelevance` and `QERWorkingStep.ComplianceRelevance`) is no longer supported.
- Starling Two-Factor Authentication and the Starling 2FA app are no longer supported as the Starling Two-Factor Authentication service was disconnected on November 1, 2022.
  - OneLogin is used for multi-factor authentication for requests or attestation.
  - Use the new functionality of adaptive cards with Starling Cloud Assistant to approve requests and attestation cases.
- The generic LDAP connector is no longer supported. Use the **LDAP Connector (version 2)**.
- The Domino connector no longer supports synchronization of the following environments:
  - IBM Domino Server versions 8, 9, and 10
  - IBM Notes Client versions 8.5.3 and 10.0

  Update your target system environment to a supported version. For more information, see Supported data systems on page 40.

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

- The following scripts are labeled obsolete. A warning to this effect is issued during compilation.
  - VI_GetValueOfObject
  - VID_GetValueOfDialogObject
  - VI_ITDataFromOrg
  - VI_AE_ITDataFromOrg
  - VI_GetOrgUnitFromCertifier
  - VI_ConvertDNToCanonicalName
  - VI_PersonAuto_LDAP
  - VI_PersonAuto_ADS
  - VI_PersonAuto_EBS
  - VI_PersonAuto_Notes
  - VI_PersonAuto_SAP
  - VI_PersonAuto_SharePoint_SPSUser
  - VI_GetAttestationObject
- In future, the Domino connector will no longer support synchronization of the following environments:
  - HCL Domino Server version 11
  - HCL Notes Client versions 11.0.1 and 12.0

System requirements

Before installing One Identity Manager 9.1.3, 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

Minimum requirements for using SQL Server as a database server

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

Processor	8 physical cores with 2.5 GHz+ frequency (non-production) 16 physical cores with 2.5 GHz+ frequency (production) NOTE: 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM (non-production) 64 GB+ RAM (production)
Hard drive storage	100 GB
Operating system	Windows operating system • Note the requirements from Microsoft for the SQL Server version installed. UNIX and Linux operating systems • Note the minimum requirements given by the operating system manufacturer for SQL Server databases.
Software	Following versions are supported: • SQL Server 2019 Standard Edition (64-bit) with the latest cumulative update • 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. • Compatibility level for databases: SQL Server 2019 (150) • Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) • SQL Server Management Studio (recommended)

NOTE: The minimum requirements listed above are 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

To manage the One Identity Manager database in a managed instance in Azure SQL Database, you require the **Business critical** tier. For more detailed information, see the Microsoft site under https://azure.microsoft.com/en-us/services/sql-database/.

Minimum requirements for clients

The following system requirements must be met on the clients.

Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	1 GB
Operating system	Windows operating systems

	Following versions are supported: • Windows 11 (x64) • Windows 10 (32-bit or 64-bit) with version 1511 or later • Windows 8.1 (32-bit or 64-bit) with the current service pack
Additional software	• Microsoft .NET Framework version 4.8 or later • Microsoft Edge WebView2
Supported browsers	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimum requirements for the Job server

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

Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project.
Additional software	Windows operating systems • Microsoft .NET Framework version 4.8 or later NOTE: Take the target system manufacturer's recommendations for connecting the target system into account.

	Linux operating system • Mono 6.10 or later

Minimum requirements for the web server

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

Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.
Additional software	Windows operating systems • Microsoft .NET Framework version 4.8 or later • Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.8 and the Role Services: • Web Server > Common HTTP Features > Static Content • Web Server > Common HTTP Features > Default Document • Web Server > Application Development > ASP.NET • Web Server > Application Development > .NET Extensibility • Web Server > Application Development > ISAPI Extensions • Web Server > Application Development > ISAPI Filters • Web Server > Security > Basic Authentication

	• Web Server > Security > Windows Authentication • Web Server > Performance > Static Content Compression • Web Server > Performance > Dynamic Content Compression Linux operating system • NTP - Client • Mono 6.10 or later • Apache HTTP Server 2.0 or 2.2 with the following modules: • mod_mono • rewrite • ssl (optional)

Minimum requirements for the application server

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

Processor	8 physical cores 2.5 GHz+
Memory	8 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems Following versions are supported: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.
Additional	Windows operating systems

software	• Microsoft .NET Framework version 4.8 or later • Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.8 and the Role Services: • Web Server > Common HTTP Features > Static Content • Web Server > Common HTTP Features > Default Document • Web Server > Application Development > ASP.NET • Web Server > Application Development > .NET Extensibility • Web Server > Application Development > ISAPI Extensions • Web Server > Application Development > ISAPI Filters • Web Server > Security > Basic Authentication • Web Server > Security > Windows Authentication • Web Server > Performance > Static Content Compression • Web Server > Performance > Dynamic Content Compression Linux operating system • NTP - Client • Mono 6.10 or later • Apache HTTP Server 2.0 or 2.2 with the following modules: • mod_mono • rewrite • ssl (optional)

Supported data systems

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

Table 56: 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.

Connector	Supported data systems
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.
Web service connector	Any SOAP web service providing wsdl. NOTE: You can use the web service wizard to generate the configuration to write data to the web service. You require additional scripts for reading and synchronizing data used by the web service connector's methods.
Active Directory connector	Active Directory shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 and Windows Server 2022.
Microsoft Exchange connector	• Microsoft Exchange 2013 with cumulative update 23 • Microsoft Exchange 2016 • Microsoft Exchange 2019 with cumulative update 1 • Microsoft Exchange hybrid environments
SharePoint connector	• SharePoint 2013 • SharePoint 2016 • SharePoint 2019 • SharePoint Server Subscription Edition
SAP R/3 connector	• SAP Web Application Server 6.40 • SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55, 7.56, 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)
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the specifications for One Identity Safeguard Authentication Services.
Domino connector	• HCL Domino Server versions 11 and 12 • HCL Notes Client versions 11.0.1 and 12.0

Connector	Supported data systems
	The 64-bit variant of Notes Client 12.0.1 is currently not supported. 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) • CData ADO.NET Provider • SAP HANA • PostgreSQL
Mainframe connector	• RACF • IBM i • CA Top Secret • CA ACF2
Windows PowerShell connector	• Windows PowerShell version 3 or later
Active Roles connector	• Active Roles 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.5, 7.5.2, 7.5.3, 7.6, 8.0, 8.1.1, and 8.1.3
Azure Active Directory connector	• Microsoft Azure Active Directory NOTE: Synchronization of Azure Active Directory tenants in national cloud deployments with the Azure Active Directory connector is not supported. This affects: • Microsoft Cloud for US Government (L5) • Microsoft Cloud Germany • Azure Active Directory and Microsoft 365 operated by 21Vianet in China For more information, see https://support.oneidentity.com/KB/312379. • Microsoft Teams
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0. They must conform to

Connector	Supported data systems
	RCF 7643 (System for Cross-domain Identity Management: Core Schema) and RFC 7644 (System for Cross-domain Identity Management: Protocol).
Exchange Online connector	- Microsoft Exchange Online
Google Workspace connector	- Google Workspace
Oracle E-Business Suite connector	- Oracle E-Business Suite versions 12.1, 12.2, and 12.2.10
SharePoint Online connector	- Microsoft SharePoint Online
One Identity Safeguard connector	- One Identity Safeguard versions 6.0, 6.7, 6.13, 7.0, 7.1, 7.2, 7.3, 7.4, and 7.5 You can find the Windows 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 Windows 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, etc).

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

Table 57: 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 (will include fixes for 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 cycle	• The product is not functioning after installing the most recent CU and the customer cannot wait until the next CU 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 9.2). 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 9.2 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 9.2, and, for example, versions 9.1.3, 9.1.4, and 9.1.5 have been released, you only have to install version 9.2 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 9.2, 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 9.1.3 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 on page 46.

Advice for updating One Identity Manager

- Test changes in a test system before you load a migration package into a production system. Use a copy of the production database for testing.
- Ensure that the administrative system user, who is going to compile the database, has a password before you update the One Identity Manager database to version

9.1.3. 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 version 8.0.x to version 9.1.3, 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.

- During installation of a new One Identity Manager database with version 9.1.3 or while updating a One Identity Manager database from version 8.0.x to version 9.1.3, you can specify whether you want to work with granular permissions at server and database level. The Configuration Wizard then creates SQL Server logins and database users with the necessary permissions for administrative user, configuration users and end users. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

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

  > NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.1.3, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.
  >
  > If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

- 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.

Updating One Identity Manager to version 9.1.3

> IMPORTANT: Note the Advice for updating One Identity Manager on page 46.

To update an existing One Identity Manager installation to version 9.1.3

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

    d. Select the **Consistency check > Run** menu item to start testing.

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

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

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

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

       > NOTE:
       >
       > - To update a One Identity Manager Active Directory Edition, switch to the **Other Products** tab and select the **One Identity Manager Active Directory Edition** entry.

    c. Click **Install**.

       This starts the installation wizard.

    d. Follow the installation instructions.

       > IMPORTANT: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.

3. Complete the One Identity Manager Service on the update server.

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

5. Check whether the database's compatibility level is set the **150** and change it if necessary.

6. Run the One Identity Manager database schema update.

    - Start the Configuration Wizard on the administrative workstation and follow the instructions.

      Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.

        - Use the same user as you used for initially installing the schema.
        - If you created an administrative user during schema installation, use that one.
        - If you selected a user with Windows authentication to install the schema, you must use the same one for updating.

      > NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.1.3, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

> If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

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

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

        > IMPORTANT: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.
8. Check the login information of the One Identity Manager Service. Specify the service account to use.
9. Start the One Identity Manager Service on the update server.
10. Update other installations on workstations and servers.

    You can use the automatic software update method for updating existing installations.

To update synchronization projects to version 9.1.3

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.

    For more information, see Applying patches to synchronization projects on page 52.

To update an application server to version 9.1.3

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

To update the Web Designer Web Portal to version 9.1.3

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

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

To update an API Server to version 9.1.3

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

To update the Operations Support Web Portal to version 9.1.3

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

To apply changes from version 9.1.3 to your HTML applications

1. Load the current source code from the One Identity Github repository.
2. Pull the changes from the **v91** branch into your repository.
3. Compile your HTML application and fix any compilation errors that may occur.

   For more information, see the *One Identity Manager HTML5 Development Guide*.
4. Check whether you HTML application still work properly.
5. Deploy the new version of your HTML application.

   For more information, see the *One Identity Manager HTML5 Development Guide*.

To update the Manager web application to version 9.1.3

1. Uninstall the Manager web application
2. Reinstall the Manager web application.

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

Applying patches to synchronization projects

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

Before you apply a patch

1. Read the patch description to decide whether it provides the necessary improvements for the synchronization project.
2. Check whether conflicts with customizations could occur.
3. Create a backup of the database so that you can restore the original state if necessary.
4. (Optional) Deactivate the synchronization project.

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

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

To apply patches

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Edit > Update synchronization project** menu item.
3. In **Available patches**, select the 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:

- Modified synchronization templates on page 20
- Patches for synchronization projects on page 22

Verifying successful installation

To determine if this version is installed

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

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

  The version number 2022.0009.0001.0300 for all modules and the application version 9.1 v91-251054 indicate that this version is installed.

Additional resources

Additional information is available from the following:

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

Globalization

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

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

The release is localized in the following languages: German

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

About us

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

Contacting us

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

Technical support resources

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

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

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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