One Identity Manager 9.1.1

Release Notes

17 April 2023, 11:10

These release notes provide information about the One Identity Manager release version 9.1.1. You will find all the modifications since One Identity Manager version 9.1 listed here. For the most recent documents and product information, see Online product documentation.

One Identity Manager 9.1.1 is a minor release with new functionality and improved behavior. See New features on page 2 and Enhancements on page 4.

If you are updating a One Identity Manager version older than One Identity Manager 9.1, read the release notes from the previous versions as well. You will find the release notes and the release notes about the additional modules based on One Identity Manager technology under One Identity Manager Support.

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

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

About One Identity Manager 9.1.1

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

With this product, you can:

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

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 9.1.1:

General

- Support for SQL Server 2022 with compatibility level **SQL Server 2019 (150)** for databases.

Target system connection

- Now you can configure how the system handles group memberships of user accounts if the user accounts are linked to employees but do not use account definitions. Define the behavior in the **QER | Person | User | KeepMembershipsOfLinkedAccount** configuration parameter.
- Support for Oracle E-Business Suite version 12.2.10.
- Support for One Identity Safeguard version 7.1.

- Support for Secure Password Extension Password Manager Version 5.11.1.
- Active Roles version 8.1.1 is supported.

Identity and Access Governance

- Support for Behavior Driven Governance for OneLogin. This includes:
  - Attestation and recertification of OneLogin application access. Assignments can be removed automatically after attestation is denied.
  - Identification of user accounts and applications that have not been used for a given period. Recertification of these assignments is started automatically. This identifies OneLogin roles that were used to assign the applications. Assignments are removed automatically if attestation is denied. The time period is stored in the **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** configuration parameter.
  - User accounts that have not been used for a defined period can be identified. The required behavior is set up in the **TargetSystem | UNS | UnusedUserAccountThresholdInDays** configuration parameter.
  - Identification of applications assigned to more than one OneLogin role, and OneLogin roles that grant access to more than one application.

  NOTE: To use behavior driven governance, events with types 5, 6, 7, 8, 11, 22, 29 must be synchronized. To accelerate synchronization and reduce the number of entries in the change history, you can customize the scope of the `Event` schema type.

  To change the scope

  1. In the Synchronization Editor, open the synchronization project.
  2. In the navigation view, select **Configuration > Target system**.
  3. Select the **Scope** view.
  4. Click **Edit scope**.
  5. Select the **Event** schema type.
  6. Select the System filter tab and extend the existing filter definition as follows:

     ```
     event_type_id=5,6,7,8,11,22,29&since=$olgeventsincefilter$
     ```
  7. Save the changes.
- In Microsoft Teams, you can attest teams and team memberships. Default attestation policies and default approval workflows are provided for this. There is support for automatic removal of team memberships if attestation is denied.
- The authorization definition of an SAP function can be formulated such that all the permitted values of an authorization object must exist in order to match the SAP function. To do this, all the values to be tested are concatenated into a list delimited with + in the authorization definition.

- Compliance rule properties extended for integrating with Easy Content Solution from IBS Schreiber. This allows the predefined Easy Content Solution rules to be imported into One Identity Manager and applied to the existing data.

See also:

- Enhancements on page 4
- Resolved issues on page 8
- Schema changes on page 35
- Patches for synchronization projects on page 38

Enhancements

The following is a list of enhancements implemented in One Identity Manager 9.1.1.

Table 1: General

Enhancement	Issue ID
Improved resetting of slots if the Database Agent Service causes processing errors.	35792
Improved spell checking of object keys.	35457
Improved performance when processing DBQueue Processor tasks.	36408
Improved performance of process handling.	35068, 36091
Improved help in command line tools.	35657
The Configuration Wizard displays an improved error message when selecting an existing database if the database's name contains illegal characters.	35643
Additional examples of Docker files for target systems now under https://github.com/OneIdentity in the Docker Files Repository.	34992
Improved documentation about the initial password in password policies.	35711
Improved documentation of language settings for database users.	35623
The trusted source key can be set for Docker containers.	36341
New optional parameter `/alive` in the `DatabaseAgentServiceCmd.exe` command line program for monitoring the status of the Database Agent Service. The status is checked on a 15-minute cycle.	36276
Auto-completion when writing scripts can now be enabled or disabled via an icon.	35895, 36479

Enhancement	Issue ID
The Data Import preferentially maps columns with identical names if the source columns and target columns are mapped automatically.	36047
Improved performance when generating triggers for change tracking.	35961
In the Docker container for the API Server, it now possible to connect a History Database.	36553
Improved support for manually setting the trusted source key in web applications.	36198
Improved treatment of attributes in the SCIM plugin.	36542

Table 2: General web applications

Enhancement	Issue ID
The Password Reset Portal does not display detected password policy violations as script errors.	35236
The Dojo Toolkit has been updated to version 1.17.3.	387671, 36188
The NPM packages have been updated.	385798
Requests from the API documentation (Swagger) no longer fail due to the missing X-XSRF-TOKEN header, as it is now included in the requests.	394255
Improved security of the web applications.	403744
Improved Web Portal performance.	36038, 36229, 392694

Table 3: Target system connection

Enhancement	Issue ID
Various functions required to manage a OneLogin domain are now provided in the Manager. It is now possible to: • Create account definitions for domains • Define exclusion of roles • Specify administrators for roles • Use the various reports on offer	35909
The list of permitted values for group claims of Azure Active Directory app registrations has been extended.	36441
Descriptions of Azure Active Directory policies can now be over multiple lines.	36442

Enhancement	Issue ID
Improved performance synchronizing Azure Active Directory user accounts.	35877
The BAPI transport SAPTRANSPORT_70.ZIP is also deployed as a Workbench transport for systems that do not support Unicode.	35460
Improved mapping of external identifiers (SAPUserExtID). A patch with the patch ID VPR#35991 is available for synchronization projects.	35991
The list of Google Workspace products and SKUs was updated.	36175
Consistency checks are provided to test a system synchronization's configuration.	34371
Errors migrating synchronization projects can now be better identified and handled. • Migration errors are shown in the synchronization project. • If migration failed with an error (entry in DPRShell.LastMigrationError), changes to the synchronization project can now be saved. • The error message contains a reference to the patch that causes the error.	35773
Improved error message if synchronization unexpectedly quits.	36358
A single retry for loading single objects with the SCIM connector has now been implemented.	34740
Improved performance loading mailboxes in the Microsoft Exchange connector.	35175
Direct modifications of the RSECUSERAUTH table without maintaining the RSECUSERAUTH_CL change log that belongs to it in the /VIAENET/RSECUSERAUT_ADD and the /VIAENET/RSECUSERAUT_DEL functions, have been converted to the existing function modules in the SAP R/3 system (RSEC_ASSIGN_AUTHS_TO_USERS_DYN and RSEC_DELETE_AUTHS_FROM_USERS).	35917
Improved performance of SharePoint Online synchronization by optimizing the SharePoint Online connector.	35975
To allow the target system owners for SAP R/3 to handle outstanding objects, viewing permissions have been issued to the Person, Department tables, and the tables for synchronizing SAP authorization objects. To allow the target system owners for Oracle E-Business Suite to handle outstanding objects, viewing permissions have been issued to the Person, Department, PersonInDepartment, Locality, and PersonInLocality tables.	35269
In synchronization projects for synchronizing external databases with the	34088

Enhancement	Issue ID
generic database connector, it is now possible to configure how to handle data that is not allowed in Microsoft .NET Framework and thus cannot be mapped in One Identity Manager.	
When setting up a synchronization project for a cloud application with the SCIM connector, the endpoint configuration data can be stored locally.	35698
Improved performance saving new synchronization projects in the project wizard.	35873
Optimized verification of object mapping rules in the Synchronization Editor. This displays any failed objects.	35959
Improved performance in the synchronization engine.	35687
The Synchronization Editor saves backup copies of scripts when they are being debugged.	35704
The maximum number of attempts at synchronizing failed objects can be set in the start up configuration.	34432
In the synchronization workflow, you can configure whether additional testing takes place if conflicts occur due to simultaneous handling of objects in the target system.	36472
A workaround has been implemented for the missing UI support for encrypted connections of the SAP HANA ADO.NET provider.	35828
Improved documentation of the permissions required for registering an enterprise application for One Identity Manager in the Azure Active Directory tenant.	36385

Table 4: Identity and Access Governance

Enhancement	Issue ID
Improved displaying of samples and policy collections in the **Attestation** category of the Manager.	35844
Attestation runs that were not completed due to processing errors can be canceled in the Manager and then restarted.	35566
Improved performance recalculating approvers for IT Shop requests.	33934, 35600
Improved delegation performance if the original approver needs to be notified.	36023
In the Manager, multi-request resources are displayed in the request history under **Approved requests**.	36504
The **ReducedApproverCalculation** configuration parameter is now considered when determining the fallback approver.	36483

See also:

- Schema changes on page 35
- Patches for synchronization projects on page 38

Resolved issues

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

Table 5: General

Resolved issue	Issue ID
If data imported via a CSV connector uses an application server connection, the default values of properties cannot be removed.	34584
In the Schema Extension, a summary of the changes is no longer shown.	35075
Using the emergency stop to halt the DBQueue Processor can result in a time delay if a lot of DBQueue Processor processes are being handled quickly.	35338
WebView2 is not installed on administrative workstation if only **Workstation | Configuration** or **Workstation | Development & Testing** machine roles are selected.	35709
The Form Editor generates an empty form definition when a new interface form is inserted in the form overview's root level.	35910
Permissions required on new tables are not granted for end users if the Database Transporter imports the schema extensions.	35934
The `QBM_PTriggerDrop` procedure logs entries in the system journal even though no triggers were deleted.	35949
An error occurs in the Manager using the context menu to run a task is run on an object.	35952
An error occurs updating statistics during maintenance tasks. Therefore, the statistics are not up-to-date. Error message: `User does not have permission to perform this action.`	35960
The Manager does not reliably save the column selection in a filter.	35965
An error occurs when the Software Loader imports a new file. Error message: `Number of primary key columns does not match.`	36006
An error occurs using OAuth2.0/OpenID Connect to log in to the application server or the Job server, to display the status, for example.	36018
The Job Queue Info does not display the change information for the	36103

Resolved issue	Issue ID
`CausingEntityPatch` parameter correctly.	
Hierarchically structured changes labels are not displayed correctly in the Database Transporter when transporting by change label.	36115
If the functionality for read access distribution in a cluster is used, a message appears stating that the Database Agent Service is not running although it was started.	36120
Some SQL statements that only query data still require a database connection with write access. Under certain conditions, errors can occur when read access distribution is used in the cluster.	36137
The `QBMColumnLimitedValue.KeyValue` column is too short.	36146
The Process Editor cannot restore the default layout.	36149
Schema extensions do not populate existing data records with default values. This causes errors.	36176
Rule violations are not identified in the simulation.	36181
After ending a simulation, the data is not fully displayed in the report.	36182
Special change labels are not displayed when changes are committed in the Designer.	36190
An error occurs on saving in the Designer if a change label was selected that already contains references to objects.	36208
Running the `ExecuteTemplates` method on a multi-select object does not return a result.	36223
Entries in a list of permitted values may not be translated correctly.	36225
Error running the **Check uniqueness of alternate keys** consistency check.	36250
The `ProcID` parameter is not taken into account in triggered processes with the `FireGenEvent` process task of the `HandleObjectComponent` process component.	36255
The Database Transporter does not display each transport of a cumulative transport correctly.	36262
Multiple start times for a schedule are not taken into account correctly when calculating the run times and while running.	36263
The Schema Extension creates indexes for object keys (`XObjectKey`) whose names are more than 30 characters long and therefore do not comply with the naming convention.	36269
Machine roles are not correctly applied in the Docker container for the API	36277

Resolved issue	Issue ID
Server.	
If the server function for a process step changes, the system does not notice that the process needs to be recompiled.	36281
If a schedule is supposed to run on a certain day of the week, an error occurs when calculating the next run.	36287, 36290
An error occurs loading collections with an empty where clause.	36304
An error occurs when an export definition that is saved in the user settings is deleted in the Manager.	36365
Filter queries for menu items that contain objects with certain starting characters are run too often.	36405
The Job Queue Info throws an error when the number of retries is set.	36462
Under certain conditions, such as when the network is interrupted, the Database Agent Service plugin stops and does not start again.	36469
Under certain conditions, the Database Transporter compiles web projects too often when it imports a cumulative update.	319014
Columns that do not exist in certain tables are queried in the transport condition.	35351
The Configuration Wizard does not process calculation tasks for the DBQueue Processor when a database is restored.	35876, 36428
Auxiliary tables are not included in consistency checks.	36186
The One Identity Manager Service status page is not always shown.	36381
Error running the `QBM_PJobCreate_HOInsert` procedure if a **WhereClause** property changes.	36062
Process steps in the Job queue sporadically have an inconsistent state and cannot be processed.	36382
Custom triggers might be deleted when the One Identity Manager database is updated from version 8.1.x to version 9.1.	36607
The import of custom schema extensions checks references to columns before the columns themselves are imported.	36326
If a column was marked for recording historical data in the source database but is removed again before it is transferred to the History Database, the History Database transfer fails.	36205
In certain cases, an error occurs sending subscribed reports.	36273
HTTP-HEAD requests to the One Identity Manager Service website cause the	36320

Resolved issue	Issue ID
following error: `"Bytes to be written to the stream exceed the Content-Length bytes size specified."`.	
Processes on the `DialogDatabase` table can no longer be started manually. This also affects the `ATT_DialogDatabase_Trigger_AttestationCase_VerificationMail` process.	35572
In the database query with the **Historical assignments** query module, the user shown as the `CreateUser` is not the one that created the assignment.	35946
Permissions filters are modified by code processing.	36177
Error creating a generating condition or a script for a process using dollar ($) notation if a foreign key column is selected by double-clicking the right mouse button.	36434
The Database Transporter does not show data that causes a conflict correctly in the **Merge conflict** dialog box.	36637
Error saving requests if processes are already in the Job queue that can trigger events to send mail for other requests. Error message: `String or binary data would be truncated in table 'OneIM.sys.TT_QBM_YParameterList_6A941822', column 'Parameter1'.`	36622
Under certain conditions, exporting to the History Database fails.	36516
It is only possible to install a module with the Configuration Wizard later if another module is selected for update at the same time.	36429
If parallelization of process handling is intensive, the Job queue can enter an inconsistent state when processes are restarted.	36367
Processes that are not run because the `IsExclusivePerObject` process task is enabled, can stop other processes from running.	35802
Replacing variables from the navigation in element descriptions on overview forms does not work.	36683
After reindexing tables as part of maintenance tasks, not all indexes may be released again.	36292

Table 6: General web applications

Resolved issue	Issue ID
You cannot upload a profile image in the Web Portal.	34425
In the Web Designer Web Portal, it is not possible to request a multi-requestable/unsubscribable resource for an identity more than once.	34743
The wrong information is shown when logging in to the Web Designer Web Portal.	35057

Resolved issue	Issue ID
Under certain conditions, the scrollbars are missing in the Password Reset Portal.	35535
Under certain conditions, the Web Designer Web Portal always prompts that too many search results were found.	35759
Under certain conditions, the Web Portal search function does not return the expected result.	35826
In the Web Portal, the shopping cart implies you can send a subset of the requested items.	35898
The modified **Display pattern** property does not affect the request or request parameters in the Web Portal.	35899
If you enter a date for a product property in the Web Portal's shopping cart, under certain conditions the value is deleted when the shopping cart is submitted.	35995
The Web Designer Web Portal does not display all the tiles correctly.	36015
The Web Portal search does not return the correct results if an asterisk (*) is included as a placeholder.	36032
In the Web Designer Web Portal, you must enter a product's request parameters for each request recipient although the product is configured such that the request parameters only have to be entered once.	36066
Under certain conditions in the Web Designer Web Portal, you cannot export the request history data.	36095
Too many database connections are established in the Web Designer Web Portal for unauthorized queries.	36116
The Web Portal does not display new requests immediately in the respective tile.	36117
The Web Designer Web Portal does not check renewal requests and cancellations correctly in the shopping cart.	36131
Under certain conditions, dependencies of multiple request parameters to one another are not taken into account in the Web Portal.	36143
Code highlighting and auto completion of variables does not work in the Web Designer.	36145
An error can occur when the Manager web application is automatically updated.	36193
Under certain conditions, the Web Designer Web Portal does not show a change icon when values are added or changed.	36230
Under certain conditions, selecting requests and displaying the request	36316,

Resolved issue	Issue ID
history in the Web Portal, can lead to long response times for administrators of organizations and business roles.	36613
In the Web Portal, it is only possible to manage directly subordinate identities.	36325
Under certain conditions, the Web Portal's request history shows request properties with the incorrect values.	36357
Under certain conditions in the Web Portal, it is not possible to create service items for system entitlements.	36377
In a customized Web Portal, you cannot add a product renewal as a request to the shopping cart.	36616
In the Web Portal, the request workflow displays withdrawal of an additional approver incorrectly.	292577
In the Web Portal, the shopping cart uses the wrong product names.	317017
In the Web Portal, the **Request details** pane does not appear anymore once products are added to the shopping cart that require more information.	317218
The Web Portal displays some untranslatable text when the terms of use are being accepted.	318203
The Web Portal displays the wrong message when selecting requestable products if a product was already assigned.	319133
The Web Portal does not display memberships that were added or deleted in system roles in an identity's history.	319462
If you make a new request in the Web Portal using a peer group, the products selected by organizational structure are each put in their own shopping cart.	320891
Under certain conditions, installing the Web Portal fails.	320955
In the Operations Support Web Portal a column title is not translated correctly in the process overview.	321613
Under certain conditions, instead of the display name the Web Portal displays only the ID of the selected object when conditions for automatic membership are created.	321874
The Web Portal does not always show the correct results when grouping and filtering in tables at the same time.	322124
Under certain conditions, the Web Portal shows the splash screen all the time.	322907
Under certain conditions, the Password Reset Portal shows the splash screen all the time.	322939

Resolved issue	Issue ID
In the Web Portal, when you reset objects to their previous state you can switch to the second step in the wizard without entering data. This causes an error.	322985
The Operations Support Web Portal leaves the queue list empty, and no data appears.	323845
In the Web Portal, it is not possible to search by compliance rules and to filter the respective search results.	323899
In the Web Portal, no recipient must be selected if requesting for others.	324118
In the Web Portal, no system role memberships are displayed.	324128, 36503
The Web Portal uses the wrong identifiers in the details of an attestation case.	324279
Under certain conditions, after clicking **Assign/Change** in the Web Portal, no objects can be selected for property fields.	324289
It is not possible to create new user accounts in the Password Reset Portal.	324290, 36034
The Web Portal shopping cart does not correctly display whether an identity is not entitled to request a product. The request can still be sent, but it has no effect.	324383
The Web Portal marks all pending requests as compliance violations the moment just one of the displayed pending requests causes a compliance violation.	326083
The Web Portal cannot display a compliance violation in the shopping cart and the respective shopping cart cannot be submitted.	326440
A report is not subscribable in the Web Portal if it is not configured for PDF format.	326723
It is not possible to edit identity main data in the Web Portal, even if you have all the necessary permissions.	330766, 36011
In the Web Portal, it is not possible to publish application entitlements.	332393
In the Web Portal, the **Requests submitted by other users** filter option in the request history does not work.	332423
If you change the title of a web application is causes follow-up problems.	352481, 36016
In the Web Portal, copying attestation policies causes an error.	358311, 36090
Under certain conditions, errors occur when displaying potential rule viola-	366940

Resolved issue	Issue ID
tions in the shopping cart.	
In the Web Portal, requesting a product causes an error if the product cannot be requested for at least one request recipient.	367180
In the Web Portal, it is possible to add products in the shopping cart although the recipient does not have request authorization.	367187
In the Web Portal, approval decisions about policy violations can only be made once.	367251
The Web Designer Web Portal does not display all the tiles on the request page correctly.	367316
The Web Portal does not translate the descriptions of the corresponding company policies correctly when it displays policy violations.	367441
Under certain conditions, the **View Settings** menu in the Web Designer Web Portal is shown twice.	367741, 35722
If you try to log in to the Web Portal with the wrong credentials, an empty page is displayed instead of an error message.	384912
In the Administration Portal, the links to some of the web applications are incorrect.	386166
Under certain conditions, the Operations Support Web Portal does not display provisioning processes.	386554
Under certain conditions, it is not possible to add products to request templates in the Web Portal.	386663
Under certain conditions the Web Portal does not load data correctly when requests for products with additional information are made.	386868
Under certain conditions, an error occurs editing the date fields.	387324, 36166
In the Web Portal, you cannot display the details of request templates.	388710
The Web Designer Web Portal header is displayed incorrectly.	389051
The Operations Support Web Portal does not translate all the user interface captions of the **Pending provisioning processes** function correctly.	389068, 36362
In the Web Portal, it is not possible to assign new attestation policies to policy collections.	390235, 36414
Renewed login to a web application again does not change the `imx_sessiongroup` cookie.	393075, 36317
In the Administration Portal, it is not possible to disable the **Service items without image inherit the image of the assigned service category**	393570

Resolved issue	Issue ID
configuration key.	
Grouping attestation cases in an attestation run's details in the Web Portal causes an error.	393864, 36359
Under certain conditions, password questions cannot be edited in the Web Portal.	395047
Under certain conditions, the numerical values of the following configuration parameters are not read in correctly. • QER\ITShop\Recommendation\ApprovalRateThreshold • QER\ITShop\Recommendation\PeerGroupThreshold • QER\ITShop\Recommendation\RiskIndexThreshold • QER\ITShop\PeerGroupAnalysis\ApprovalThreshold	400775
The API Server sometimes uses invalid connections to the application server.	36495
It is not possible to log in to the Administration Portal using OAUTH authentication.	36360
In the Web Portal, attestation cases offered to identities for approval although their approval is not required anymore.	36505, 405092
The Web Portal displays a number instead of a string for the **Gender** property in the details of an attestation run.	36529
In certain cases in the Web Portal, issues with business roles that conflict with each other are not found when the shopping cart is checked.	36533

Table 7: Target system connection

Resolved issue	Issue ID
The SCIM connector sets boolean and numerical properties to `null` if they do not contain a value. Error message: `Cannot convert null to 'bool' because it is a non-nullable value type.`	34609
On Windows Server 2012, the Exchange Online connection fails to connect to the target system.	34807
On the **Define search criteria for employee assignment** form in the Manager, the Google Workspace user accounts are not shown when a new search criterion is defined.	34853
Error editing the endpoint configuration of a system connection to a cloud application.	34957
The display values of multi-value properties are not shown properly in the target system browser.	34959

Resolved issue	Issue ID
Azure Active Directory synchronization generates too many processes.	35018
An error occurs when an Azure Active Directory group is created without an alias.	35180
Error connecting to a database via the generic database connector if the password for the database login contains double quotes.	35409
Error copying synchronization projects.	35453
Error creating a synchronization project for synchronizing Oracle E-Business Suite. Error message: `An item with the same key has already been added.`	35541
Microsoft Exchange remote mailboxes are not included when determining the origin of entitlements.	35589
The Active Directory connector writes structural objects classes for domains (`ADSDomain.StructuralObjectClass`) at every synchronization. A patch with the patch ID VPR#35808 is available for synchronization projects.	35808
User accounts (`UNSAccount`) without containers (`UNSContainer`) are ignored even if there are not any containers in the target system.	35823
If Active Directory is synchronized using a special variable set, an error occurs when Active Directory SIDs are updated by the `MaintainOtherSid` process task.	35824
Under certain conditions, an error occurs simulating synchronization: • Simulation is run over a remote connection. • Simulation is started several times for the same start up configuration.	35857
Error saving a synchronization project if the connection goes through the application server and the target system connection has high network latency. Error message: `Application server returned an error.`	35871
If an object filter was defined for a root entry in the scope definition, there might not be an object in the scope.	35880
Synchronization with OneLogin fails if there are self-registered users. Error: `Null object cannot be converted to a value type.`	35889
The target system alignment uses an incorrect formatter option.	35907
If there are several redundant entries in SAP R/3 for an authorization object, only one authorization definition is read into the One Identity Manager	35944

Resolved issue	Issue ID
database when SAP authorization objects are synchronized. All other instances are ignored. In particular, the instance with the highest value is missing. A patch with the patch ID VPR#35944 is available for synchronization projects.	
Error loading SharePoint Online objects if an object filter is defined.	35947
Access to the **RemoteConnectPlugin** does not work across machines. The HTTP server registration has been adjusted and can be set up using the **HttpAuthentication** and **HttpBindAddress** parameters in the plugin's configuration.	35950
An error occurs loading the list of all Active Directory user accounts with the Active Directory connector if one of the user accounts contains a mistake.	35953
Synchronization with OneLogin might possibly report ambiguous keys in the reference resolution to the `OLGUserHasOLGCustomAttribute` table.	35962
References that cannot be allocated because the OneLogin objects no longer exist, are saved in the synchronization buffer. A patch with the patch ID VPR#35969 is available for synchronization projects.	35969
You cannot select an account definition on the OneLogin user account's master data form.	35983

Processing conflicts between synchronization and other system processes (for example, provisioning) are not always reliably detected.
In the StdioProcessor configuration file, the rate of updating the processing information can now be configured. By default, the data remains in the cache for **60** seconds. Only change this value if there is an issue.
If you are affected by the issue, add the following entries to the `StdioProcessor.exe.config` file:
`<configSections>`
`...`
`<section name="synchronization" type="System.Configuration.NameValueSectionHandler" />`
`...`
`</configSections>`
`<synchronization>`
`<add key="SysConcurrenceCacheLifeTime" value="60" />`
`</synchronization>`
	35992

Resolved issue	Issue ID
The **OLG_4_NAMESPACEADMIN_ONELOGIN** permissions group has too many edit permissions on OneLogin applications (`OLGApplication` table) and OneLogin roles (`OLGRole` table).	35994
An error occurs if a synchronization project is created for Azure Active Directory and provisioning of subscription assignments (`AADUserHasSubSku` table) is disabled.	35997
The schema provided by the Domino connector might be incomplete or individual properties might not have the correct data type.	35644, 35999, 36142
There is no recalculation of the effective assignments of target system-specific system entitlements if the inheritance settings defined in the manage level are overwritten. The following assignments are affected: • Subscription assignments to Azure Active Directory user accounts (`AADUserHasSubSku` table) • Entitlement assignments to Oracle E-Business Suite user accounts (`EBSUserInResp` table) • Role assignments to SAP R/3 user accounts (`SAPUserInSAPRole` table) • Structural profile assignments to SAP R/3 user account (`SAPUserInSAPHRP` table)	36014
There is no recalculation of the effective assignments of system entitlements for cloud target systems if the inheritance settings defined in the manage level are changed.	36020
The `O3SWeb.Description` column is too short.	36025
Provisioning processes in a target system go into a **Frozen** state if a password containing special characters is transferred with encryption.	36043
There is no recalculation of the effective assignments of system entitlements for custom target systems if the inheritance settings defined in the manage level are changed.	36045
An error occurs in the One Identity Safeguard connector if tags are used in object filters.	36063
Error changing an employee's default email address if they have an Azure Active Directory user account with an Exchange Online mailbox.	36088
When a synchronization project is created over a remote connection, an error can occur during deserialization.	36089
A synchronization simulation quits unexpectedly if a remote connection is used.	36092
`PATCH` operations generated for schema extension properties cause an error	36108

Resolved issue	Issue ID
in the SCIM connector. A patch with the patch ID VPR#36108 is available for synchronization projects.	

In the Synchronization Editor, the timeout for a remote connection is too short. For example, this can cause errors when creating a synchronization project over a remote connection.
The timeout has been increased to 3 minutes to solve the issue. If this timeout is not sufficient, you can adjust the following value in the `SynchronizationEditor.exe.config` file.
`<remoting>`
`<add key="RequestTimeout" value="180" />`
`</remoting>`
	36112

When a synchronization project is created over a remote connection, an error can occur if the volume of data is too big.	36123
If the One Identity Manager database is encrypted, the system mistakenly encrypts the `ExpirePassword` connection parameter in synchronization projects with the LDAP connector for IBM RACF.	36136
A scope filter configured hierarchically in a connected LDAP target system with a Microsoft implementation (Active Directory Lightweight Directory Service (AD LDS) or Active Directory) has no effect.	36141
Ineffective memberships in cloud groups or system entitlements are provisioned. A patch with the patch ID VPR#36150 is available for synchronization projects.	36150
The Manager does not display the menu item for user accounts and groups of cloud target systems correctly.	36155
In the `UNSAccount` proxy table, the `AccountName` column for the `EX0MailBox`, `EX0MailContact`, and `EX0MailUser` tables is empty.	36163
An error occurs when the Synchronization Editor performs a consistency check on schedules with multiple start times.	36164
Errors can occur when writing the synchronization log.	36168
Connecting to an Azure Active Directory tenant with schema extensions for types that are not currently supported by the Azure Active Directory connector ("device" for example) causes an error. Error message: `Object reference not set to an instance of an object.`	36170
Dynamic memberships of Azure Active Directory user accounts in Office 365	36180

Resolved issue	Issue ID
groups that are marked as outstanding cannot be deleted by target system synchronization.	
A conversion error occurs for `Oracle.ManagedDataAccess.Types.OracleDecimal`' when objects in a table are added in a sequence.	36195
If a scope file was defined, an error occurs adding new objects with the SCIM connector because of an incorrect query.	36211
Single roles contained in collective roles cause errors with double entries in the One Identity Manager database when synchronizing SAP role assignments to user accounts in a CUA.	36218
In the Synchronization Editor, the start up configuration list that can be assigned to a start up sequence is empty.	36226
It is not possible to select an account definition for the Active Directory domain on the Microsoft Exchange mailbox or the Exchange hybrid remote mailbox forms.	36228, 36257
It is not possible to delete a SharePoint Online site collection with an assigned administrator (`O3SSite.UID_O3SUserPrimaryAdmin`).	36232
No OneLogin user accounts can be assigned to employees.	36241
Certain SAP communication data such as preferred telephone numbers or preferred email addresses that are marked as outstanding, cannot be deleted during target system synchronization.	36264
Error displaying schema types in the target system browser of a SAP HCM system's synchronization project if a hierarchy is defined that contains a circular reference.	36270
No passwords are transferred to the LDAP target system if the LDAP connector V2 is being used. A patch with the patch ID VPR#36271 is available for synchronization projects.	36271
It is possible that new objects do not display meaningful values if they were incompletely mapped.	36283
An error occurs updating LDAP synchronization projects. Error message: `Error running the Apply' script of patch (VPR#33513 - Support multiple domains with the same DN)!`	36286
The **ADS_PersonHasTSBAccountDef_Autocreate_ ADSAccount/Contact** process goes into a **Frozen** state in the **Wait until dependent objects recalled** process step.	36298
If errors occur loading target system objects, synchronization quits even	36311

Resolved issue	Issue ID
though the workflow has the **Continue on error** option enabled.	
Using the `O3S_CreateO3SSite` script to add SharePoint Online site collections does not work if modern authentication with a certificate is used.	36322
The DBQueue Processor removes Active Directory user accounts from Active Directory groups that have the **Read-only memberships** property (`ADSGroup.HasReadOnlyMemberships`).	36327
The target system browser for Exchange Online objects sometimes displays GUIDs instead of readable values.	36330
The Azure Active Directory connector sends unnecessary (empty) patches after a group is updated where only members or owners have changed.	36345
The filters generated in the SCIM connector for resolving references are not formatted correctly.	36347
LDAP user accounts and groups cannot be deleted if they are connected to a SharePoint user account.	36354
Active Directory user accounts and groups cannot be deleted if they are connected to a SharePoint user account.	36354
Unnecessary updates are triggered by the LDAP connector if there are empty values.	36372
Filters in the SCIM connector may not contain sufficient data to query objects in the target system.	36379
Virtual properties for resolving references attempt to use the synchronization buffer in target systems.	36392
Error provisioning object changes if the `DPRProjectionObjectState` table contains object references with the `System.Byte[]` object type. Error message: `The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or an illegal character among the padding characters.`	36399
It is not possible to enter multiple lines of encrypted data in the Synchronization Editor.	36440
The **User account is disabled** property for user accounts (`LDAPAccount.AccountDisabled`) is not taken into account in the LDAP connector V2. A patch with the patch ID VPR#36450 is available for synchronization projects.	36450
Process steps for setting permissions and publishing are not carried out if the home directory of Active Directory user accounts with unknown home directory paths is moved.	36470

Resolved issue	Issue ID
Provisioning assignments of SAP BI user account to BI analysis authorizations takes a very long time and sends a lot of RFC queries to the SAP application server.	36474
An error occurs creating the **Send as** and **Full access** mailbox permissions for Microsoft Exchange remote mailboxes.	36456
An error occurs when multiple custom target system user accounts or groups are selected in the Manager.	36512
Authentication via **WindowsHttpAuthentication** does not work in the One Identity Manager Service.	36552
Under certain conditions, processes that should be exported together to a History Database are not grouped into a process group.	36438
Error during delta synchronization of Azure Active Directory group memberships.	36481
The target system's own cross-site scripting tokens are not sent to the SCIM provider in the header of a write operation.	34554
If the `InternetAddress` schema property is empty, a warning is written in the system journal when HCL Domino is synchronized (not initial synchronization). A patch with the patch ID VPR#35816 is available for synchronization projects.	35816
The value in the `AADUser.ThumbnailPhoto` column is not provisioned in the target system.	36586
Changes to the Microsoft Exchange mailbox databases in One Identity Manager are overwritten by old values. A patch with the patch ID VPR#36151 is available for synchronization projects.	36151
Error synchronizing a cloud application with the SCIM connector when filters are defined in the synchronization project.	36590
Error loading objects if a schema extension for an SAP R/3 synchronization project has a key property defined that is longer that 70 characters.	36491
Error provisioning assignments of SAP BI analysis authorizations to BI user accounts if assignment is across clients.	36518
Sometime the calculation of assignment from cloud user accounts to cloud groups fails.	36404
Error generating the synchronization log if a new value contains a very long string.	36630

Resolved issue	Issue ID
Error loading objects lists via remote connections.	36128
Error provisioning a new Microsoft Teams team.	36682
When memberships are removed from Unix groups, other memberships that should not be removed are deleted.	36679

Table 8: Identity and Access Governance

Resolved issue	Issue ID
Under certain conditions, entries in the `PWOHelperPWO` table are not recalculated.	35972
Duplicate entries in the `AttestationHelper` table. Sporadically, entries are created twice in the auxiliary table for attestation cases (`AttestationHelper`). This means the number of email notifications is doubled. If the approval workflow contains an approval step for external approval, the process for external approval is generated twice.	36000
Permissions missing from the **vi_4_ITSHOPADMIN_OWNER** permissions group for the columns `ADSGroup.HasReadOnlyMemberships` and `AADGroup.HasReadOnlyMemberships`.	36078
Application entitlements that are created automatically might not have a display name.	36094
The `CreateITShopOrder` method for creating assignment requests for memberships in Exchange Online mail-enabled distribution groups is missing.	36160
The `TSBVPersonAndGroups` view can contain duplicates. For example, this can cause errors generating reports about the origin of entitlements.	36187
If the display pattern for the `Person` table is customized such that the `InternalName` column is not used anymore, errors occur when generating email notifications for the next approver.	36214
Office 365 groups are not taken included when determining the origin of entitlements.	36217
The Analyzer cannot run an analysis after the database connection has changed.	36253
If the **QER | ITShop | ExceededValidUntilUnsubscribe** configuration parameter is set, unsubscribing processes quit unexpectedly with an error.	36274
Under certain conditions, those responsible for organizations are not deleted. • An application role is assigned to a department as an additional manager.	36301

Resolved issue	Issue ID
• An employee becomes a member of this application role by assignment request. • The assignment is canceled. However, the employee remains manager of the department (entries in the `HelperHeadOrg` table with `XOrigin = 8` are not deleted).	
End users are missing edit permissions for the `AttestationHistory` table.	36302
If an approval decision is made when a request is created, no email notification is sent to the requester.	36318
Error attesting objects with properties that are disabled by a pre-processor conditions.	36370
Too many recalculation tasks are generated by removing the mutually exclusive entry from Active Directory groups.	36079
The Analyzer does not run without an error.	36197
Attestation procedures are loaded too often if users have limited permissions.	35862
An error occurs if multiple attestation runs are created simultaneously for an attestation policy. Only one attestation run is created. The processes to generate further attestation runs fail.	36364
Error attesting if the attestation was delegated and the length of the text in the reason for the approval decision is longer than 400 characters.	36267
If identifiers were issued manually in the working copy of a rule, incorrect identifiers are formed for compliance rules and subrules (`UID_ComplianceRule` and `UID_ComplianceSubRule`) when compliance rules are enabled.	36266
DBQueue Processor requests `CPL-K-ComplianceSubRuleFillPersonS` block each other, are reset repeatedly, and are not processed.	36297
An error occurs running the **System entitlement ownership attestation** default attestation policy.	32864
The permissions to edit a dynamic role's role/organization in the Manager are wrong.	36106
Given values are not in permitted in the approval sequence for the affected approval's type (`PWODecisionHistory.DecisionType`).	35015
If there is no employee assigned to the product owner application roles, they will be deleted even if they are assigned to a service item or service category.	36421
If a shopping cart with request parameters is sent off and the request is	34993

Resolved issue	Issue ID
automatically approved because the **QER | ITShop | DecisionOnInsert** configuration parameter is set, the request parameters are missing from the request procedure.	
If request parameters are given for a request, the UIDs are displayed in the request history instead of the parameters' display names.	36207
When requests are canceled because the requested product has been removed from the IT Shop, the request recipients are not notified, although a mail template, Cancel, is stored with the approval policy.	35616
Sporadically, there are double entries in the auxiliary table for request procedures (`PWOHelperPWO`).	36139
Error assigning service items to Azure Active Directory groups marked with the **Read-only memberships** property (`ADSGroup.HasReadOnlyMemberships`).	36528
Approval procedures stop responding when the number of approvers is set to **-1**.	36443
In the Manager, multiple pending requests cannot be canceled at the same time.	36490
Error calculating memberships in dynamic roles: `The current transaction cannot be committed and cannot support operations that write to the log file.`	36531
If the product owner of a service item in an Azure Active Directory group changes, the members of the originally assigned application role remain as group owners. If the product owner of a service item in an Exchange Online e-mail enabled distribution group changes, the members of the originally assigned application role remain administrators of the distribution group.	35064
Events on the `Person` base object are not generated properly if management of an employee's role memberships (like the primary department) is automated via IT Shop requests.	36614
If a customer is removed from a shop in which they have requests and this customer is authorized to request the same product in another shop, then the changes are not illustrated clearly in the approval history.	35058

See also:

- Schema changes on page 35
- Patches for synchronization projects on page 38

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 9: General

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

Known Issue	Issue ID
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

Table 10: Web applications

Known Issue	Issue ID
The error message `This access control list is not in canonical form and therefore cannot be modified` 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.	32938

Known Issue	Issue ID
• In the Web Designer, change the **Filter for subscribable reports** configuration key (**VI_Reporting_Subscription_Filter-RPSSubscription**) and set the schedule's **Minimum character count** value (`UID_DialogSchedule`) to **1**.	

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

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

Table 11: Target system connection

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use `Import-PSSession` internally.	23795
By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely. 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

Known Issue	Issue ID
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. • Add a custom column to the table `SAPUser`. • Extend the SAP schema in the synchronization project by a new schema type that supplies the required information. • Modify the synchronization configuration as required.	27359
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	796028,

Known Issue	Issue ID
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.	30963
Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled. Cause: The SharePoint connector loads all object properties into cache by default. Solution: • Correct the error in the target system. - OR - • Disable the cache in the file `VI.Projector.SharePoint.<Version>.Host.exe.config`.	31017
If a SharePoint site collection only has read access, the server farm account cannot read the schema properties `Owner`, `SecondaryContact`, and `UserCodeEnabled`. Workaround: The properties `UID_SPSUserOwner` and `UID_SPSUserOwnerSecondary` are given empty values in the One Identity Manager database. This way, no load error is written to the synchronization log.	31904

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

Known Issue	Issue ID
n, sapnco, Version=3.0.0.42, Culture=neutral, PublicKeyToken=50436dca5c7f7d23" /> </sectionGroup> • In the new section: <SAP.Middleware.Connector> <GeneralSettings anyDateTimeValueAllowed="true" /> </SAP.Middleware.Connector>	
There are no error messages in the file that is generated in the PowershellComponentNet4 process component, in OutputFile parameter. Cause: No messages are collected in the file (parameter OutputFile). The file serves as an export file for objects returned in the pipeline. Solution: Messages in the script can be outputted using the *> operator to a file specified in the script. Example: Write-Warning "I am a message" *> "messages.txt" Furthermore, messages that are generated using Write-Warning are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an Exception. This message then appears in the One Identity Manager Service's log file.	32945
The Google Workspace connector cannot successfully transfer Google applications user data to another Google Workspace user account before the initial user account is deleted. The transfer fails because of the Rocket application's user data. Workaround: In the system connection's advance settings for Google Workspace, save a user data transfer XML. In this XML document, limit the list to the user data to be transferred. Only run the Google applications that have user data you still need. For more information and an example XML, see *One Identity Manager Administration Guide for Connecting to Google Workspace*.	33104
In the schema type definition of a schema extension file for the SAP R/3 schema, if a DisplayPattern is defined that has another name in the SAP R/3 schema as in the One Identity Manager schema, performance issue may occur. Solution: Leave the DisplayPattern empty in the schema type definition. Then the object's distinguished name is used automatically.	33812

Known Issue	Issue ID
If target system data contains appended spaces, they go missing during synchronization in One Identity Manager. Every subsequent synchronization identifies the data changes and repeatedly writes the affected values or adds new objects if this property is part of the object matching rule. Solution: Avoid appending spaces in the target system.	33448
The process of provisioning object changes starts before the synchronization project has been updated. Solution: Reactivate the process for provisioning object changes after the `DPR_Migrate_Shell` process has been processed.	
After an update from SAP_BASIS 7.40 SP 0023 to SP 0026 or SAP_BASIS 7.50 SP 0019 to SP 0022, the SAP R/3 connector can no longer connect to the target system.	34650

Table 12: Identity and Access Governance

Known Issue	Issue ID
During approval of a request with self-service, the `Granted` event of the approval step is not triggered. In custom processes, you can use the `OrderGranted` event instead.	31997
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 unsubscribes anymore. Solution: Create a process for the `AccProduct` base object that is triggered when changes are made to `AccProduct.MaxValidDays`. The process calculates the 'valid until' date for these requests (`PersonWantsOrg.ValidUntil`) from `PersonWantsOrg.ValidFrom` and `AccProduct.MaxValidDays`. After which, you can unsubscribe the requests.	36349

Table 13: Third party contributions

Known Issue	Issue ID
Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting **File and Printer sharing** is	24784

Known Issue	Issue ID
not set on the server. This option is not set on domain controllers on the grounds of security.	
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
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...'`	33026

Known Issue	Issue ID
`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.	

Schema changes

The following provides an overview of schema changes from version 9.1 up to version 9.1.1.

Configuration Module

- The `QBMColumnLimitedValue.KeyValue` column was extended to `nvarchar(256)`.

Target System Base Module

- The data type of the `UNSAccountInUNSGroup.XIsInEffect` column was changed to `bit`.

Active Directory Module

- The data type of the `ADSVAccountInADSGroup.IsMembership`, `ADSVAccountInADSGroup.IsPrimary`, and `ADSVAccountInADSGroup.XIsInEffect` columns was changed to `bit`.
- The data type of the `ADSVMachineInADSGroup.IsMembership`, `ADSVMachineInADSGroup.IsPrimary`, and `ADSVMachineInADSGroup.XIsInEffect` columns was changed to `bit`.

SharePoint Online Module

- The `O3SWeb.Description` column was extended to `nvarchar(max)`.

SAP R/3 User Management module Module

- The data type of the `SAPVSAPUserInSAPRoleAll.XIsInEffect` column was changed to `bit`.

Identity Management Base Module

- The data type of the `QERVPersonHasElement.XIsInEffectOfPersonAssignment` column was changed to `bit`.

Compliance Rules Module

- New columns `ComplianceRule.RiskDescription`, `ComplianceRule.RiskObjectives`, `ComplianceRule.RiskOrgMitigationCtrl`, and `ComplianceRule.RiskScope` for extending compliance rules.

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 up to version 9.1.1. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 64.

Modified synchronization templates

The following provides you with an overview of modified synchronization templates. Patches are made available for updating synchronization templates in existing synchronization projects. For more information, see Patches for synchronization projects on page 38.

Table 14: Overview of synchronization templates and patches

Module	Synchronization template	Type of modification
Target System Synchron-ization 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	changed
Active Roles Module	Synchronize Active Directory domain	none

Module	Synchronization template	Type of modification
	via Active Roles	
Cloud Systems Management Module	Universal Cloud Interface synchronization	changed
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)	changed
Google Workspace Module	Google Workspace synchronization	none
LDAP Module	AD LDS synchronization	None
	AD LDS Synchronization (version 2)	changed
	OpenDJ synchronization	None
	OpenDJ Synchronization (version 2)	changed
	Generic LDAP Synchronization (version 2)	changed
	Oracle DSEE Synchronization (version 2)	changed
Domino Module	Lotus Domino Synchronization	changed
Exchange Online Module	Exchange Online synchronization (v2)	None
Microsoft Teams Module	Microsoft Teams (via Azure Active Directory)	None
OneLogin Module	OneLogin Domain Synchronization	changed
Privileged Account Governance Module	One Identity Safeguard synchronization	none
SAP R/3 User Management module Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	none
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	none
SAP R/3 Compliance Add-on	SAP R/3 authorization objects	changed

Module	Synchronization template	Type of modification
Module		
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	none
	SCIM synchronization	none
Unix Based Target Systems Module	Unix Account Management	none
	AIX Account Management	none

Patches for synchronization projects

The following is a list of all patches provided for synchronization projects in One Identity Manager 9.1.1. Every patch contains a script, which tests whether the patch can be applied to the synchronization project. This depends on the specific configuration of the synchronization.

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

Table 15: 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 16: Patches for Microsoft Exchange

Patch ID	Patch	Description	Issue ID
VPR#36151	Correction of	Corrects the property mapping rule for	36151

Patch ID	Patch	Description	Issue ID
	property mapping rules for `Mailbox database` and `Archive mailbox database`	`Mailbox database` and `Archive mailbox database` in the `Mailbox` mapping, to prevent changes to mailbox databases in One Identity Manager being overwritten by old values. This patch is applied automatically when One Identity Manager is updated.	

Table 17: 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 18: 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 19: 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 20: Patches for SAP R/3

Patch ID	Patch	Description	Issue ID
VPR#35991	Correction of property mapping rules in the `userExternalID` mapping	Sets the **Force mapping against direction of synchronization** option on various property mapping rules in the `userExternalID` mapping. This patch is applied automatically when One Identity Manager is updated.	35991

Table 21: 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 22: 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 23: 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 24: General patches

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

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

Table 25: 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	Adds a property mapping rule for the `CreationType` schema	35290

Patch ID	Patch	Description	Issue ID
	type of Azure Active Directory user accounts.	property to the `Group` mapping. This patch is applied automatically when One Identity Manager is updated.	
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 26: 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 27: Patches for Active Roles

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

Table 28: 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 29: 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.	34265

Patch ID	Patch	Description	Issue ID
		This patch is applied automatically when One Identity Manager is updated.	
VPR#34766	Support for certificate-based authentication	Adds the `AADOrganization` variable to the default variable set. This patch is applied automatically when One Identity Manager is updated.	34766
VPR#35343_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 30: 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 31: 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 32: Patches for LDAP

Patch ID	Patch	Description	Issue ID
VPR#35702	Ignore upper and lower case when comparing	Sets the **Ignore case** option in the property mapping rules of the `ObjectClass` and `StructuralObjectClass`	35702

Patch ID	Patch	Description	Issue ID
	values	schema properties. This patch is applied automatically when One Identity Manager is updated.	
	Milestone 9.1	Milestone for the context **LDAP**.	

Table 33: 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 34: 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 35: 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

Patch ID	Patch	Description	Issue ID
	Milestone 9.1	Milestone for the context **Privileged Account Management**.	

Table 36: Patches for SAP R/3

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

Table 37: 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 38: 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 39: Patches for SAP R/3 authorization objects

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

Table 40: Patches for SharePoint

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

Table 41: 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 42: 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 43: 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 44: Patches for Unix

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

Table 45: Patches for the One Identity Manager connector

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

Table 46: Patches for the CSV connector

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

Deprecated features

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

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

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

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

- The generic LDAP connector is no longer supported. Use the **LDAP Connector (version 2)**.

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

- The following 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

System requirements

Before installing One Identity Manager 9.1.1, 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 47: 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	• IBM Domino Server versions 8, 9, and 10 • HCL Domino Server versions 11 and 12

Connector	Supported data systems
	• IBM Notes Client 8.5.3 and 10.0 • HCL Notes Client versions 11.0.1 and 12.0 The 64-bit variant of Notes Client 12.0.1 is currently not supported. 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, and 8.1.1
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

Connector	Supported data systems
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0. They must conform to RCF 7643 (System for Cross-domain Identity Management: Core Schema) and RFC 7644 (System for Cross-domain Identity Management: Protocol).
Exchange Online connector	• Microsoft Exchange Online
Google Workspace connector	• Google Workspace
Oracle E-Business Suite connector	• Oracle E-Business Suite versions 12.1, 12.2, and 12.2.10
SharePoint Online connector	• Microsoft SharePoint Online
One Identity Safeguard connector	• One Identity Safeguard versions 6.0, 6.7, 6.13, 7.0, and 7.1 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.

Product licensing

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

Upgrade and installation instructions

To install One Identity Manager 9.1.1 for the first time, follow the installation instructions in the *One Identity Manager Installation Guide*. For detailed instructions about updating, see the *One Identity Manager Installation Guide*.

IMPORTANT: Note the Advice for updating One Identity Manager on page 59.

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 9.1.1. Otherwise the schema update cannot be completed successfully.
- For One Identity Manager databases on SQL Servers, it is recommended, on performance grounds, that you set the database to the **Simple** recovery model for the duration of the schema update.
- During the update of a One Identity Manager database version 8.0.x to version 9.1.1, different columns that were already semantically defined as mandatory fields become physical mandatory fields.

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

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

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

  UPDATE fails
  ```

  Check and correct data consistency before updating a One Identity Manager database. In the add-on for the Configuration Module on the installation medium, a test script (`\SDK\SQLSamples\MSSQL2K\30374.sql`) is provided. In case it fails, correct the data and restart the update.
- One Identity Manager uses In-Memory OLTP ((Online Transactional Processing) for memory optimized data access. The database server must support Extreme Transaction Processing (XTP). If XTP is not enabled, the installation or update will not start. Check whether the SQL Server property **Supports Extreme Transaction Processing** (IsXTPSupported) is set to **True**.

  The following prerequisites must be fulfilled to create memory-optimized tables:

  - A database file with the file type **Filestream data** must exist.
  - A memory-optimized data filegroup must exist.

  The Configuration Wizard checks whether these prerequisites are fulfilled before the One Identity Manager database can be installed or updated. The Configuration Wizard offers repair methods for creating the database file and database group.
- During the update, calculation tasks are queued in the database. These are processed by the DBQueue Processor. Processing calculation tasks may take some time depending on the amount of data and system performance.

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

Therefore, ensure that you have configured an appropriate procedure for archiving the data before you update the database. For more information about archiving data, see the *One Identity Manager Data Archiving Administration Guide*.

- For the period of the update, the database is set to single user mode. Close all existing connections to the database before starting the schema update.
- You may experience problems activating single-user mode when using database mirroring.
- During installation of a new One Identity Manager database with version 9.1.1 or while updating a One Identity Manager database from version 8.0.x to version 9.1.1, you can specify whether you want to work with granular permissions at server and database level. The Configuration Wizard then creates SQL Server logins and database users with the necessary permissions for administrative user, configuration users and end users. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

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

  NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.1.1, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

  If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.
- After the update has completed, the database switches automatically to multi-user mode. If this is not possible, you receive a message in which you can manually switch to multi-user mode.
- Once this version has been installed, users that need to access the REST API in the application server require the **Enables access to the REST API on the application server** (`AppServer_API`) function. Assign this program function to the users. For more information, see the *One Identity Manager Authorization and Authentication Guide*.

Updating One Identity Manager to version 9.1.1

IMPORTANT: Note the Advice for updating One Identity Manager on page 59.

To update an existing One Identity Manager installation to version 9.1.1

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

    All the database tests must be successful. Correct any errors. Some consistency checks offer repair options for correcting errors.
2. Update the administrative workstation, on which the One Identity Manager database schema update is started.
    a. Run the `autorun.exe` program from the root directory on the One Identity Manager installation medium.
    b. Change to the **Installation** tab. Select the Edition you have installed.

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

    c. Click **Install**.

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

    IMPORTANT: On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.
3. Complete the One Identity Manager Service on the update server.
4. Make a backup of the One Identity Manager database.
5. Check whether the database's compatibility level is set the **150** and change it if necessary.
6. Run the One Identity Manager database schema update.
    - Start the Configuration Wizard on the administrative workstation and follow the instructions.

      Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.
        - Use the same user as you used for initially installing the schema.
        - If you created an administrative user during schema installation, use that one.

- If you selected a user with Windows authentication to install the schema, you must use the same one for updating.

NOTE: If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to version 9.1.1, use an installation user with permissions for this permissions concept. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

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

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

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

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

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

To update synchronization projects to version 9.1.1

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 64.

To update an application server to version 9.1.1

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

To update the Web Designer Web Portal to version 9.1.1

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

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

To update an API Server to version 9.1.1

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

To update the Operations Support Web Portal to version 9.1.1

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

To update the Manager web application to version 9.1.1

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 36
- Patches for synchronization projects on page 38

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 2022.0009.0001.0100 for all modules and the application version 9.1 v91-201110 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