# One Identity Manager 8.1.1

# Release Notes

**July 2019**

These release notes provide information about the One Identity Manager release, version 8.1.1. You will find all the modifications since One Identity Manager version 8.1 listed here.

One Identity Manager 8.1.1 is a patch release with new functionality and better behavior. See New features on page 3 and Enhancements on page 6.

If you update a One Identity Manager version that is older that One Identity Manager 8.1, 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 8.1.1

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 concern with One Identity Manager

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

## One Identity Hybrid Subscription

The newest version of our on-prem products will offer a mandatory One Identity Hybrid Subscription, which helps our customer's transition to a hybrid environment on their way to the cloud. The subscription enables you to join their on-prem solutions with our One Identity Starling software-as-a-service platform. Giving your organization immediate access to a number of cloud-delivered features and services, which expand the capabilities of your on-prem product. We will continuously make available new products and features to our One Identity SaaS platform. With the One Identity Hybrid Subscription, you can use these immediately for their One Identity on-prem solutions and their subscription continues to add value.

Expand the capabilities of One Identity Manager with One Identity Hybrid Subscription, which offers a myriad of additional cloud-delivered features and services. Gain access to all-you-can-eat Starling Two-Factor Authentication to protect administrative access, to enforce additional factor authentication when requesting or approving critical access or to enable out of band user verification for password requests. For an additional cost, these offerings can also be extended to additional target systems and use cases. A single subscription can be used for all your One Identity products.

# New features

New features in One Identity Manager 8.1.1:

## Basic functionality

- Support for managed instances in Azure SQL Database.

  Operating the One Identity Manager database in a managed instance in an Azure SQL Database requires the **Business critical** tier.

  For detailed information about demands on a managed instance in an Azure SQL Database in One Identity Manager, see the *One Identity Manager Installation Guide*. For detailed information about the pricing, visit Microsoft's https://azure.microsoft.com/en-us/services/sql-database/ website.
- Windows Server 2019 is supported for service, web and application servers.
- Use the **Common | MailNotification | DefaultFont** and the **Common | MailNotification | DefaultFontSize** configuration parameters to specify font and font size for mail templates in the Mail Template Editor.
- In mail templates, any parameters can be used when calling a script.

  Syntax: `$SCRIPT(ScriptName, "Options")$`

  The `Options` parameter is optional and is passed as a `string`. Custom parameters can be coded in any way in this string. Quotes ("") are masked by doubling. In the script, the parameter is passed as the second parameter after the base object. The base object can now be either `IEntity` or `ISingleDbObject`.
- The **RequestWatchDogPlugin** has a new **Action** parameter (`Action`) to specify which action should be run when queries come to a still stand. Permitted values are **Restart** (default) and **Log**.

## Web applications

- One Identity now offers users the option to log in, simply and securely, to One Identity Manager web applications with help of (physical) security keys. These security keys support the W3C standard **Webauthn**. Using them guarantees a high degree of login security.

  New Web Designer configuration keys:

  - VI_Common_AccessControl_Webauthn_2FAID
  - VI_Common_AccessControl_Webauthn_2FA_VisibleControls
  - VI_Employee_QERWebAuthnKey_Filter
  - VI_Common_AccessControl_Webauthn_2FA

  For detailed information, see the *One Identity Manager Web Portal User Guide*, the *One Identity Manager Web Application Configuration Guide* and the *One Identity Manager Identity Management Base Module Administration Guide*.

- It is now possible, with the help of three Web Designer configuration keys, to specify the format of date and time input for the entire web project.

  New Web Designer configuration keys:

  - VI_Common_InputFormat_DateTime
  - VI_Common_InputFormat_Date
  - VI_Common_InputFormat_Time

  For more information about value formats, see https://docs.telerik.com/kendo-ui/framework/globalization/dateformatting.
- The terms of use are now automatically shown in the same language as the Web Portal.

## Target system connection

- You can now synchronize departments and the employees assigned to them using synchronization projects for employee data from an Oracle E-Business Suite Human Resources module. To do this, two new mappings are provided with the default synchronization template.

  In addition, the Oracle E-Business Suite connector also supports hierarchy filters for organization hierarchies. In the synchronization project's scope, departments you want to synchronize can be filtered from all the organizations by using the hierarchy filter.

  Departments can also be differentiated from other organizations by their type. As you can customize these types in Oracle E-Business Suite, departments are not filtered by type in the default mappings. To filter departments by type, define your own schema class.

  > NOTE: The new default mappings are only available in synchronization projects that have been created with One Identity Manager 8.1.1. There is no patch for this change.
  >
  > To apply this functionality to existing synchronization projects, update the target system schema in these projects. This makes two new schema types available, `HROrganization` and `HRPersonInOrganization`. Define your own schema classes for these schema types and your own mappings.
- Support for One Identity Safeguard version 2.6 and Version 2.7.

  Patches with the patch IDs VPR#31459, VPR#31664A, VPR#31664B, VPR#31703, VPR#31775A and VPR#31775B are available for synchronization projects.
- Improved support of One Identity Safeguard clusters when establishing a connection.

  A patch with the patch ID VPR#31569 is available for synchronization projects. If you use One Identity Safeguard clusters, run the system connection wizard after applying the patch, to determine the cluster's appliances.
- Initially, approvers of access request policies automatically become owners of PAM assets, PAM asset accounts, PAM directory accounts, PAM asset groups and PAM

account groups. This assignment only takes place if an access request policy can be determined for a PAM object. For each access request policy, a new application role is created for the owner under the **Privileged Account Governance | Asset and account owners** application role.

An application role for owners is only assigned automatically to a PAM object if an application role is not already assigned to the PAM object. Any existing assignment is not changed. You may change the application role manually.

- Microsoft Exchange 2019 with cumulative update 1 and Microsoft Exchange 2016 cumulative update 12 are supported.
- Microsoft Exchange linked room mailboxes are supported.

  A patch with the patch ID VPR#30964 is available for synchronization projects.
- One Identity Manager supports the disbanding of an SAP R/3's central user administration. The central user administration and child systems can be removed so that they subsequently become independent clients, which can be managed by One Identity Manager and administrated separately from each other.

  Not only can single clients be removed from the central user administration but the entire central user administration can be disbanded.

  Ask support for instructions about disbanding the central user administration. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.
- A recertified version of the One Identity Manager Business Application Programming Interface (BAPI) is available. The BAPI has reduced functionality, which works to the advantage of performance. The BAPI is no longer compatible with One Identity Manager version 6.1.x or older versions.

  The BAPI's functions are available as an Add-On Assembly Kit (AAK) package, a transport package from copies and now also as a Workbench transport package. You can chose any import path. Coding is identical.
- SharePoint 2019 is supported.
- Execution of provisioning and single object synchronization processes as well as target specific processes can be distributed over different servers. This accelerates the entire process because objects can be handled in parallel.

  Distribution covers all servers that are assigned the server function stored in the base object.

  For detailed information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide* and the individual target system manuals.
- **TECH PREVIEW ONLY**: A new LDAP connector **LDAP Connector (Version 2 - Tech Preview)** is available. No maps and no project templates are made available with it. The connector can be tested in a test environment. You must definitely not use the connector in a live environment.

### Identity and Access Governance

- Support for a peer group analysis for requests.

  There is a new event, `PeergroupAnalysis`, for the `PersonWantsOrg` table, which can be linked into the approval workflow with an **EX** step. The event checks the hit rate within the request recipient's peer group and/or for mismatching functional areas of the requested permissions and the recipient's department. The hit rate and mismatching functional areas are registered in the request and the step is then completed after either granting or denying approval depending on the result.

  The peer group analysis configuration uses the **QER | ITShop | PeerGroupAnalysis** configuration parameter and its child configuration parameters.

See also:


- Enhancements on page 6
- Resolved issues on page 10
- Schema changes on page 27
- Patches for synchronization projects on page 30


# Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.1.1.

**Table 1: General known issues**

| Enhancement | Issue ID |
|---|---|
| Improved performance checking columns in the `QBMUniqueGroup` table that must be unique by definition. | 31263, 31648 |
| Improved performance in DBQueue Processor. | 31293 |
| Improved performance processing transactions that repeatedly queue tasks in the DBQueue. | 31490 |
| In the configuration parameter **Common \| MailNotification \| Signature \| LinkDisplay**, you can specify an alternative display text for the link to your company's website for use in email signatures. | 19852 |
| Improvements in Job Queue Info.<br>• The port is taken into account when a Job server log is displayed.<br>• A user and user password can be entered over the **Enter request credentials** context menu item to query Job server status. | 22926, 30711 |

| Enhancement | Issue ID |
|---|---|
| Support for the System Debugging on 64-bit systems. | 31203 |
| Improved login checks. Using the **Common \| Authentication \| SessionsPerUserAndMinute** configuration parameter, you can specify the number of sessions a user can open within a short space of time. The default value is **10**. If this number is exceeded, the user is sent a message. | 31321 |
| Use the configuration parameter **QBM \| DBQueue \| GenProcIDReplaceLimit** to define a limit for process replacements. | 31423 |
| Third-party components update. | 31443, 31444, 31446, 31318 |
| Improved security for the One Identity Manager Service API. | 31542 |
| Improved protection of the application server's API. | 31553, 31564 |
| Improved protection against damaging SQL statements. | 31652 |
| Improved performance in the `vQBM_PGUIDReplaceLight` procedure. | 31676 |

**Table 2: General web applications**

| Enhancement | Issue ID |
|---|---|
| In the Web Portal, all the application roles a person is responsible for are managed under **Responsibilities \| My Responsibilities \| One Identity Manager application roles**. | 797112 |
| In the Web Portal, under **My profile \| Contact data \| Language for value formatting**, users can specify how dates and numbers are formatted. | 796853 |
| Improved error message if there is no approval policy available for delegating. | 30656 |
| To prevent user sessions being stolen, the session ID is no longer given in the HTML code. The web application must run in Release mode for this. | 31656 |
| Improved security for dealing with column filters. | 31754 |

**Table 3: Target system connection**

| Enhancement | Issue ID |
|---|---|
| Improved performance reloading objects from the database. | 31404 |

| Enhancement | Issue ID |
|---|---|
| If the option **Ignore undefined values** is set for a schema property, a message appears in the synchronization log if the connector tries to write a non-defined value. | 30522 |
| Operation for memberships are recorded with more detail in the synchronization log. | 31851 |
| If the connector schema in a synchronization project was extended by using a schema extension file, the schema extension can be viewed and edited in the target system wizard after it has been saved. | 31773, 31833 |
| Access restrictions for the Azure Active Directory `User.CompanyName` schema property has been removed. `CompanyName` can now be written to.<br>A patch with the patch ID VPR#31456 is available for synchronization projects. | 31456 |
| Improved grouping of Azure Active Directory user accounts in the Manager. | 31803 |
| Improved performance provisioning Active Directory groups, containers and domains.<br>A patch with the patch ID VPR#31419 is available for synchronization projects. | 31419 |
| Improved performance by correcting object filters in Active Directory project templates.<br>A patch with the patch ID VPR#31792 is available for synchronization projects. | 31792 |
| The behavior of Active Directory processes has been changed with respect to load balancing of processes for provisioning and single object synchronization as well as target system specific processes on different Job servers.<br>NOTE: The `ADS_GetQBMServer` script was also changed in connection with this. Check your customized use and overwrites of this script.<br>If you customized the `ASD_GetQBMServer` script, it will still be run but without the load balancing function. If you want to use load balancing, customize the script accordingly or use the default script. | 30886 |
| Improved performance loading synchronization objects from Microsoft Exchange if revision filtering is used.<br>A patch with the patch ID VPR#31165 is available for synchronization projects. | 31165 |
| Improved performance loading synchronization objects from Exchange Online if revision filtering is used.<br>A patch with the patch ID VPR#31166 is available for synchronization projects. | 31166 |
| Improved performance provisioning Notes policies and certificates.<br>A patch with the patch ID VPR#31420 is available for synchronization projects. | 31420 |

| Enhancement | Issue ID |
|---|---|
| Improved performance provisioning SAP user accounts.<br>A patch with the patch ID VPR#31412 is available for synchronization projects. | 31412 |
| Improved performance deleting memberships in SAP roles. | 31235 |
| Improved split algorithm in the SAP connector if WHERE clauses in external schema extensions are very long. | 31834 |
| The LDAP connector support schema with Base64 coded content. | 28647 |
| The LDAP connector supports reading of auxiliary class attributes that were assigned in the `object class` schema through the `auxiliaryClass` attribute. | 31483 |
| The LDAP connector is more tolerant toward entries that are not RFC compliant.<br>This means that unmasked leading and trailing space characters, which do not conform to RFC 4514, are handled as insignificant, meaning they do not belong to the name anymore. All space characters that were disallowed according to RFC, are now normalized. Other non RFC compliant entries are ignored and warning written to the log.<br>NOTE: On your own LDAP systems, write operations on non RFC compliant entries result in errors. | 31548, 31873 |
| The RACF connector supports the auxiliary class `RacfUserCsdataSegment`. | 31356 |
| The process function `RunAgent` of the process component `NDO Component` has been extended by an additional parameter of type **OUT**. | 31030 |
| The **TargetSystem \| SAPR3 \| Accounts \| CalculateLicence** configuration parameter can be used to specify whether to calculate SAP system measurement for SAP user accounts. | 31204 |
| Improved performance synchronizing SAP cost centers. | 31543 |
| Improved performance by correcting object filters in SAP project templates.<br>A patch with the patch ID VPR#31796 is available for synchronization projects. | 31796 |
| The SCIM connector supports passing of the specified scope for the token requested by OAuth 2.0.<br>A patch with the patch ID VPR#31756 is available for synchronization projects. | 31756 |
| Improved performance by correcting scope filters in Oracle E-Business Suite project templates.<br>A patch with the patch ID VPR#31794 is available for synchronization projects. | 31794 |

**Table 4: Identity and Access Governance**

| Enhancement | Issue ID |
|---|---|
| Improved process monitoring of requests. The configuration parameter **Common \| ProcessState \| UseGenProcIDFromPWO** controls whether the GenProcID of an IT Shop request is retained for the entire approval process. | 31418 |
| The documentation for inheriting company resource through system roles and the effect of exclusion definitions has been comprehensively reworked ().*One Identity Manager System Roles Administration Guide* | 28312 |
| Improved performance processing requests of approvers that are automatically approved. | 31341 |
| Improved performance deleting customers with requests, from the IT Shop. | 31668 |
| Improved performance moving requests. | 31597 |
| The reminder interval and the timeout for attestation approval steps are checked every 30 minutes by default. The interval can be specified in the **Checks reminder interval and timeout of attestation cases** schedule. | 31383 |

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 30

# Resolved issues

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

**Table 5: General known issues**

| Resolved issue | Issue ID |
|---|---|
| The `QBM_PDBQueueOverviewFill` procedure updated the `DBQueueOverview` table too frequently. | 31217, 31296 |
| Error in DBQueue Processor handling: `Divide by zero error encountered.` | 31924, 31925 |
| Incorrect values in `DialogCountry.NumericCode`. | 31352 |
| The final line break is missing when CSV files with only one header are written. | 31556 |
| `DialogTree.ConfigurationFlags` is not customizable. | 31393 |
| The Database Compiler sets the **Waiting for compiler** status too early. The | 31408 |

| Resolved issue | Issue ID |
|---|---|
| status is not removed if the compiler quits prematurely. | |
| Environment variables in the `FileName` process parameter of the `SQLComponent` process component's `DumpResult` process function, are not replaced at runtime. | 31513 |
| Error in the German translation for DBQueue tasks. | 31117 |
| Migration fails if there are custom tables in a One Identity Manager History Database. | 31530 |
| The **CCCEditPermissions** permissions group does not own sufficient permissions to create for default tables with custom columns. | 31431 |
| In `CustomProperty` columns, @ cannot be used. | 31593 |
| The `QBM_PUserDetectByGroupList` procedure removes too many permissions groups. | 31601 |
| Error `String or binary data would be truncated` during One Identity Manager update to version 8.1. | 31617, 31663 |
| During the One Identity Manager update to version 8.1., custom triggers are deleted. | 31658 |
| In certain circumstances, the procedure `QBM_PDeleteDeep` leaves behind disabled triggers. | 31677 |
| Error executing the **GUID in primary key with invalid format** consistency check for the `JobQueueStats` table. | 31688 |
| The **QBMLock has no entry but XMarkedForDeletion is set** consistency check, does not output the table name. | 31860 |
| The **QBMLock has no entry but XMarkedForDeletion is set** and **QBMLock has entry without XMarkedForDeletion set** consistency checks return the wrong results for read-only tables. An error occurs when the repair method is run. | 31799 |
| Swagger definition in the application server's API documentation contains an unclosed XML statement. | 31713 |
| In certain circumstances, not all elements are indexed in the search index. | 31881 |
| The `CVSExport` process function of the `ScriptComponent` process component, writes a header every time. | 31731 |
| Wrong transliteration of Đ(U0110) and đ(U0111) in the `VID_TransliterateDiacritics` script. | 31737 |
| Error message in the HistoryDB Manager if entries exist in the One Identity Manager History Database for columns that are not configured for recording changes. | 31631 |

| Resolved issue | Issue ID |
|---|---|
| `Divide by zero error encountered` error running the system overview query for values **AVG latency write** and **AVG latency write TempDB**. | 31610 |
| Error saving a newly added script in the One Identity Manager database using the System Debugger. | 31786 |
| The `@ColumnName` variable in `QBM_ZSplittedLookupFill` is too short for `DialogColumn.ColumnName` with a length or 29 or 30 characters. | 31840 |
| It is possible to assign a new object to the generation base object (entity) during process generation.<br>NOTE: If you have used this functionality, error messages are outputted during process compilation. Correct your processes accordingly. | 31854 |
| All databases in an AlwaysOn availability group are given the same `UniqueDatabaseId`. | 31866 |
| `SingleDbObjectSnapshot` does not mask XML special characters if the value is encrypted. | 31869 |

**Table 6: General web applications**

| Resolved issue | Issue ID |
|---|---|
| Problems selecting a language if the One Identity Password Manager was started from the Web Portal. | 29035 |
| Information about the password strength is not displayed in the respective language in the Password Reset Portal. | 30694 |
| The filter settings for date columns are only available in English in the Web Portal. | 31118 |
| When a report is exported, the default template and not the custom template is used. | 31231 |
| In Web Portal, if a menu item forwards to an external URL and has the options **Open in new frame** and **Show toolbars**, the toolbar is not displayed in the popup window. | 31384 |
| If you violate the password policy whilst change a password, an error message is displayed instead of the password policy. | 30389 |
| Not all types are available in the API client's generated code. | 799497 |
| The Web Designer component **VI_Common_ExternalFormHost** has been deleted. It can no longer be used to display a any URL. If you still require this functionality, you must rebuild existing code to use the **QBM_Common_ExternalFormHost** form component. This has the advantage of not passing | 800060 |

| Resolved issue | Issue ID |
|---|---|
| URLs in the form of URL parameters. | |
| On the grounds of security, the **VI_Common_UserMessageAdd** Web Designer component now codes the given text into HTML by default. You can switch off this behavior by using the virtual function `DoNotHtmlEncode()` when the component is called. | 800062 |
| In the Web Portal, report subscriptions can be saved without a value in the mandatory field. | 31058 |
| In the Web Portal, the date is displayed in UTC format in the employee's change history. | 31434 |
| In the Web Portal, the valid until date is transferred incorrectly to the shopping cart if the time is later than 23:59. | 31484 |
| The **VI_Edit_MultiLimitedValues** Web Designer component selects values from the wrong attribute in the filter condition. | 31505 |
| The validity of a password, connecting the Password Reset Portal through the application server, is not tested until it is saved. | 31354 |
| History data from One Identity Manager version 6 is not displayed correctly in the Web Portal. | 31523 |
| Write protected values for attestation cases can be changed in the Web Portal. | 31603 |
| In certain circumstances, in the Web Portal, an error occurs when the origin of an employee's entitlement is displayed. | 31638 |
| You cannot add extensions for certain objects in the Web Designer (for example **VI_ITShop_DeleteItemFromCart**). | 31504 |
| In certain circumstances, the Web Portal freezes when exporting data. | 31295 |
| In certain circumstances, in the Web Designer, the key icon, which you click to manually establish a WCF connect, is not always visible. | 31525 |
| In certain circumstances, in the API Designer, the Database Compiler freezes during NPM processes. | 31723 |
| Very long latency in the Internet Explorer until the form for assigning a system entitlement to an owner in the Web Portal. | 31037 |
| In certain circumstances, in the Web Portal, not all product categories are displayed on the product selection page. | 31818 |
| In certain circumstances, the error `Object of type UNSAccount does not exist in database or you do not have the relevant viewing permissions` occurs during analysis of attestation cases. | 31842 |
| In certain circumstances, reports are not always displayed correctly in the | 31896 |

| Resolved issue | Issue ID |
|---|---|
| Internet Explorer and Microsoft Edge. | |
| Error sharing the default web application in release node: `The value cannot be NULL.` | 31931 |
| The grid search cannot be hidden. The value **false** for the `IsSearchActive` variable in a grid extension is not taken into account. | 31903 |
| Case sensitivity is not tested when the answer to a secret question is entered for a second time. | 31914 |

**Table 7: Target system connection**

| Resolved issue | Issue ID |
|---|---|
| Error using the Remote Connection Plugin if NTLM authentication is disabled.<br>NOTE: To correct the problem, a section, `remoting`, has been added to the Synchronization Editor's configuration file to configure usage of principle names. This modification only affects new installations. Existing installations are not changed.<br>For existing installations: If you are affected by the problem, enter the following in the `SynchronizationEditor.exe.config` file:<br>`<configSections>`<br>`...`<br>`<section name="remoting" type="System.Configuration.NameValueSectionHandler" />`<br>`...`<br>`</configSections>`<br>`<remoting>`<br>`<add key="EndpointIdentity.Type" value="" /> <!-- DNS for Domain, UPN for UserPrincipalName, SPN for ServicePrincipalName -->`<br>`<add key="EndpointIdentity.Value" value="" />`<br>`</remoting>` | 31142 |
| The correct variable set is loaded too late during synchronization startup. | 31196 |
| The synchronization log includes objects that the `Update` method has been applied to although the objects were not changed. | 31307 |
| In certain circumstances, the `DPR_Journal_CleanUp` process blocks other processes that access the synchronization log. | 31584 |

| Resolved issue | Issue ID |
|---|---|
| If synchronization deletes multiple objects and an error occurs deleting one of the objects, it is possible that not all the objects are deleted. | 31549 |
| Error processing an employee's changed memberships if the memberships are marked as outstanding. | 31570 |
| In certain circumstances, multiple mapping rules for the same property can lead to false or incomplete prototype objects. | 31702 |
| The calculation of which schema type must be loaded for scope handling, uses the wrong scope. | 31714 |
| During synchronization a method checked to see if it can be executed although the method is not allowed to be executed. This results in errors. | 31913 |
| During provisioning, no changes are written to the target system if a quota is defined in the provisioning workflow. | 31823 |
| Error loading single objects with Windows PowerShell if the parameter `Identity` is used. The error can occur, for example, during provisioning of object modifications in Exchange Online and result in follow up errors.<br>A patch with the patch ID VPR#30269 is available for synchronization projects. | 29152, 30269 |
| The Windows PowerShell consistency check does not recognize schema classes with non-unique keys. | 31324 |
| The appliance's serial number cannot be used to identify PAM appliances because the identifier is not unique.<br>Patches with patch IDs VPR#31568A and VPR#31568B are available for synchronization projects. | 31568 |
| Flag behavior inconsistent when handling `SAPComPhone.PhoneType`. | 29725 |
| Error provisioning license information for SAP user accounts in the central user administration. | 31078 |
| In Manager, departments and employee that do not originate from SAP R/3 are displayed under **Target system synchronization: SAP R/3**. | 31086 |
| In the `SAP_PersonAuto_Mapping_SAPUser` script, the wrong configuration parameter is used for automatically creating departments and no data source is passed. A new configuration parameter, **TargetSystem \| SAPR3 \| AutoCreateDepartment**, is available.<br>NOTE: If the department is loaded by SAP HCM synchronization, the configuration parameter should not be set. Otherwise, automatically generated departments are marked as outstanding. | 31226 |
| Error loading SAP user account if the name has a leading space character. | 31329 |

| Resolved issue | Issue ID |
|---|---|
| Assignments of SAP roles to user accounts with `XIsInEffect=0` are logged as deleted in the synchronization log each time synchronization is run.<br>A patch with the patch ID VPR#31427 is available for synchronization projects. | 31427 |
| On the form assigning SAP roles to SAP user accounts, outstanding or ineffective assignments are displayed in the same way as effective assignments. | 31590 |
| No objects are updated or added in the One Identity Manager database during synchronization of locations with the `HRArea` schema type from an SAP HCM system.<br>The fix corrects the mapping of the `vrtdistinguishedName` schema property. The `MOLGA` schema property is not used for mapping anymore.<br>To apply this change, update the target system schema in the synchronization project and modify the mapping. | 31642 |
| Generating a process for `SAPUserInSAPRole` creates an entry in `QBMElementAffectedByJob` for the SAP role. | 31847 |
| `SAP-K-ProfileRestriction` post-processing tasks are triggered for objects that are not SAP profiles. | 31886 |
| It is possible, if several price lists are enabled in SAP R/3 that contain a cross-section of license types, the references cannot be resolved for the SAP user account because no unique license can be assigned.<br>A patch with the patch ID VPR#31930 is available for synchronization projects. | 31930 |
| Categories for group inheritance are not displayed properly on the master data form for custom target systems. | 31563 |
| Error adding custom target system in Manager. | 31632 |
| Error accessing the SharePoint Online target system schema.<br>A patch with the patch ID VPR#31499 is available for synchronization projects. | 31499 |
| Error adding a SharePoint site collection: `Another site already exists.` | 31831 |
| If SharePoint web templates are loaded, the `vrtObjectPath` key property is made up of properties, which are not unique when combined.<br>NOTE: The first synchronization after installing this version marks existing SharePoint web templates (`SPSWebTemplate` table) as outstanding and reloads the entries. This justified because the `vrtObjectPath` key property and the distinguished name (`DistinguishedName`) have changed. The web templates marked as outstanding can be deleted. | 31837 |
| If a SharePoint site collection is in read-only mode, no access is possible, not even with the server farm account. | 31904 |

| Resolved issue | Issue ID |
|---|---|
| Changing the name of a container in Active Directory does not result in the distinguished name of sub containers changing in One Identity Manager.<br>NOTE: In the context of trouble shooting, the ADS_CreateDN script has also been corrected to map the distinguished name with masking. Check whether the script still fits your target system. You can overwrite the script if necessary. | 31596, 31751 |
| Inadequate error message if ADSSite.UID_ADSForest is empty when updating One Identity Manager to version 8.1. | 31672 |
| The CN in Active Directory can only be 64 characters long. | 31826 |
| The ADS-K-PersonHasADSGroup DBQueue Processor task create ADS-K-ADSContactInADSGroup tasks for Active Directory user accounts. | 31844 |
| In certain circumstances, the name of the forest that belongs to an Active Directory domain, cannot be determined. | 31752 |
| In certain circumstances, the ADS-K-ADSGroupInADSGroup DBQueue Processor task never completes. | 31905 |
| Error in the VI_BuildProxyAddress script. | 31783 |
| Error in the EX0_2010_EX0Mailbox_Update/Deactivate process if the Microsoft Exchange mailbox does not exist anymore in the database before provisioning. | 31535 |
| The EX0Mailbox.TotalItemSize column's display name does not match the value. | 31879 |
| Inconsistencies loading LDAP multilanguage attributes. | 31670 |
| Incorrect handling of schema properties that are marked as returned = request in the SCIM schema.<br>A patch with the patch ID VPR#31733 is available for synchronization projects. | 31733 |
| The CSM_CSMRoot_SearchandCreate_Person_PostSync process is missing. | 31864 |
| Missing scope filter for the PesonInLocality schema type in the Oracle E-Business Suite connector.<br>A patch with the patch ID VPR#31735 is available for synchronization projects. | 31735 |
| Read operation on EBSSecurityGroup causes an error.<br>A patch with the patch ID VPR#31782 is available for synchronization projects. | 31782 |
| If a synchronization project with a custom project template is created, no variables are used in the connection parameters but fixed values from the variable set. | 31739 |
| The native database connector does not support the SQL Server data type, | 31741 |

| Resolved issue | Issue ID |
|---|---|
| Datetime2. | |
| In the native database connector, the Imports VI.Projector.Database.Native import is missing in the CreateValueStore method. | 31825 |
| Error create a new password policy in the Manager. | 31495 |
| The MFRComponent process component is missing. | 31871 |
| The racfInstallationData attribute must be added in the schema for the extendable object classes racfDataset and racfResource. | 29918 |
| In certain circumstances, an error occurs while searching for RACF dataset objects. | 30587 |

**Table 8: Identity and Access Governance**

| Resolved issue | Issue ID |
|---|---|
| The description of the configuration parameter **QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveRequestedRole** is wrong. | 30481 |
| If an approval workflow is waiting for external approval and the approval step EX is reached for a different attestation object, the external approval process is restarted for all pending objects. | 30965 |
| In certain circumstances, the CreateAttestations Customizer method blocks DBQueue processing. | 31016, 31370 |
| In four Privileged Account Management specific attestation objects, the ObjectKey2 attribute contains a redundant character ("]") in the ObjectWalker notation. | 31547 |
| If a question was asked in an attestation case, the approval step might not be escalated if the time limit is exceeded. | 31571 |
| Insufficient primary key definition for the ATTVCasesOpenByPerson view. | 31667 |
| AttestationRun.HistoryNumber are not commented correctly. | 31373 |
| A request for an assignment resource by reference user does not use the approval policy that was used for the reference user. | 31234 |
| Missing Select permissions for an end user running attestation. | 31497 |
| The **Missing table assigment to PWODecisionRule for attestation** consistency check generates errors if the **ATTESTATION** pre-processor condition is not set. | 31841 |
| Error checking custom approval procedures while updating One Identity Manager to version 8.1. | 31599 |

| Resolved issue | Issue ID |
|---|---|
| Error sending email notifications if approval of an additional approver is withdrawn. | 31628 |
| The `CreateITShopOrder` method is missing for Azure Active Directory objects. | 31633 |
| You should not be able to transport the `ITShopOrg.UID_PWODecisionMethod` column because the value must be calculated. | 31705 |
| Failed process steps for IT Shop approvals do not go into the **FROZEN** status. | 31744 |
| Cancellations by the Manager without an approval workflow, are not sent an email notification.<br>To fix this problem, the default mail template **IT Shop request - canceled** has been altered. If you customized the template, test the `VI_ESS_PersonWantsOrg Send Mail when Unsubscribe` process and alter it as required. | 31759 |
| In email notifications for the IT Shop, members of the chief approval team are also displayed. | 31867 |
| The `VI_ESS_PWOHelperPWO approve anywhere` process is only generated if a mail template is entered in the approval step, | 31897 |
| Entries in the `PersonHasObject` table are not deleted when entries are deleted from the `BaseTree` table. | 31417 |
| Migration leaves behind `BaseTreeHas*` entries with `XOrigin=2`. | 31716 |
| Error calling the `ADS_ZPersonHasObject` procedure. | 31740 |
| If the `QER_ZAllForPersonInBaseTree` post-processing task has been triggered by deleting a `BaseTree` entry, the required `QER-K-AllForOnePerson` task is not generated. | 31919 |
| The calculated risk for a column is not corrected if the column does not have a risk index function anymore. | 31378 |
| Calculated risk indexes are not immediately updated after they have changed. | 31379 |
| Incorrect risk index functions. | 31337, 31395 |
| When system roles are requested, the request's compliance test does not recognize whether the compliance rule is violated by the company resources assigned to the system role. | 31430 |
| Error in the `VI_QERPolicy_QERPolicyHasObject_new violation` process if the mail template configuration parameters are not set. | 31711 |

**Table 9: IT Service Management**

| Resolved issue | Issue ID |
|---|---|
| Unsuitable sorting of call result lists. | 31392 |
| In certain circumstances during the accounting run, unique voucher items cannot mapped (`InvoiceItem` table).<br>The `InvoiceItem.DisplayName` template has been modified to fix the problem. If you have defined custom templates, which refer to voucher items, test them and modify the templates if necessary. | 31618 |

See also:

- Schema changes on page 27
- Patches for synchronization projects on page 30

# Known issues

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

**Table 10: General known issues**

| Known Issue | Issue ID |
|---|---|
| Error in the Report Editor if columns are used that are defined in the Report Editor as keywords.<br>Workaround: Create the data query as an SQL query and use aliases for the affected columns. | 23521 |
| Errors may occur if the Web Installer is started in several instances at the same time. | 24198 |
| Headers in reports saved as CSV do not contain corresponding names. | 24657 |
| In certain circumstances, objects can be in an inconsistent state after simulation in Manager. If an object is changed or saved during simulation and the simulation is finished, the object remains in the final simulated state. It may not be possible to save other modifications to this object instance.<br>Solution: Reload the object after completing simulation. | 12753 |
| Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation.<br>Cause: The Configuration Wizard was started directly. | 25315 |

| Known Issue | Issue ID |
|---|---|
| Solution: Always use `autorun.exe` for installing One Identity Manager components. This ensures that you do not select any invalid modules. | |
| Schema extensions on a database view of type **View** (for example `Department`) with a foreign key relation to a base table column (for example `BaseTree`) or a database view of type **View** are not permitted. | 27203 |
| Error connecting through an application server or the API 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`.<br>Solution: Mark the private key as exportable if exporting or importing the certificate. | 27793 |
| If a One Identity Manager database is operating in a cluster, the database is restored from a backup after a cluster failover. A new database ID is created in the process. This step cannot be missed out anymore otherwise the database cannot be compiled. | 28373 |
| It is not possible to extend predefined dynamic foreign keys by references to redefined tables. If you define custom dynamic foreign keys, at least one of the parties involved - dynamic foreign key column or referenced table - must be a custom object. | 29227 |
| Error resolving events on a view that does not have a UID column as a primary key.<br>Primary keys for objects in the 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.<br>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.<br>The consistency check **Table of type U or R with wrong PK definition** is provided for testing the schema. | 29535 |
| The default setting of `globallog.config` assumes that write access exists for `%localappdata%`. If an EXE does not have sufficient permissions, the log can be written to a directory that does have the access rights by changing the variable `logBaseDir` in the `globallog.config` or by introducing a special log configuration in the `*.exe.config` or the `Web.config` file. | 30048 |
| 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. The error, in case a `Save Transaction` is carried out is: `Cannot use SAVE TRANSACTION within a distributed transaction.`<br>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 |
| The following error occurs while the One Identity Manager database is updating from version 7.0.x, 7.1.x or 8.0.x to version 8.1.1.<br>`Database error 41337: Cannot create memory optimized tables. To create memory optimized tables, the database must have a MEMORY_OPTIMIZED_ FILEGROUP that is online and has at least one container.`<br>Cause: The user used to update the database does not have sufficient permissions.<br>Solution: Ensure that the user owns the **dbcreator** SQL Server server role. | 31981 |

**Table 11: Web applications**

| Known Issue | Issue ID |
|---|---|
| The error message `This access control list is not in canonical form and therefore cannot be modified` sometime occurs when installing the Web Portal with the Web Installer. The error occurs frequently after a Windows 10 Anniversary Update.<br>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 |

**Table 12: Target system connection**

| Known Issue | Issue ID |
|---|---|
| Memory leaks occur with Windows PowerShell connections, which use `Import-PSSession` internally. | 23795 |
| After synchronizing an SAP R/3 environment, assignments of single role to SAP user accounts are labeled as outstanding.<br>This problem can occur if:<br>• SAP role assignments to user accounts were loaded in the One Identity Manager database before installing One Identity Manager 7.0.1<br>• Single role assignments, which are included in collective roles, were mapped as direct assignments (Error ID 3218196)<br>By resolving this problem in One Identity Manager 7.0.1, incorrect assignments are labeled as outstanding after synchronizing again using the | |

| Known Issue | Issue ID |
|---|---|
| appropriate synchronization configuration.<br>Solution: Delete outstanding assignments in One Identity Manager target system synchronization. | |
| By default, the building block **HR_ENTRY_DATE** of an SAP HCM system cannot be called remotely.<br>Solution: Make it possible to access the building block **HR_ENTRY_DATE** remotely in your SAP HCM system. Create a mapping for the schema property `EntryDate` in the Synchronization Editor. | 25401 |
| Any existing secondary SIP addresses are converted into primary email addresses when Microsoft Exchange mailboxes are added, providing that no primary SIP addresses were stored up to now. | 27042 |
| The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3.<br>If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration.<br>• Add a custom column to the table `SAPUser`.<br>• Extend the SAP schema in the synchronization project by a new schema type that supplies the required information.<br>• Modify the synchronization configuration as required. | 27359 |
| No passwords can be provisioned when the `bind` method **Fast Bind** is in use in Active Directory. The `SetPassword` method is therefore not available.<br>The process step `AdhocProjection` fails with the message:<br>`[System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKNOWNNAME))).` | 27427 |
| Synchronization projects for SAP R/3 that were imported by a transport into a One Identity Manager database, cannot be opened. The problem only occurs if an SAP R/3 synchronization project was not added in the target database before importing the transport package.<br>Solution: Create and save at least one SAP R/3 synchronization project before you import SAP R/3 synchronization projects into this database with the Database Transporter. | 27687 |
| Error in IBM Notes connector (`Error getting revision of schema type ((Server))`).<br>Probable cause: The IBM Notes environment was rebuilt or numerous entries have been made in the Domino Directory.<br>Solution: Update the Domino Directory indexes manually in the IBM Notes | 27126 |

| Known Issue | Issue ID |
|---|---|
| environment. | |
| Error provisioning licenses in a central user administration's child system.<br>Message: `No company is assigned.`<br>Cause: No company name could be found for the user account.<br>Solution: Ensure that either:<br>• A company, which exists in the central system, is assigned to user account.<br>- OR -<br>• A company is assigned to the central system. | 29253 |
| Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will not come into effect until later.<br>Cause: The function `BAPI_EMPLOYEE_GETDATA` is always executed with the current date. Therefore, changes are taken into account on a the exact day.<br>Solution: To synchronize personnel data in advance that will not come into effect later, use a schema extension and load the data from the table `PA0001` directly. | 29556 |
| Error synchronizing an OpenDJ system, if a password begins with an open curly bracket.<br>Cause: The LDAP server interprets a generated password of the form `{<abc>}<def>` as a hash value. However, the LDAP server does not allow hashed passwords to be passed.<br>Solution: The LDAP server can be configured so that a hashed password of the form `{<algorithm>}hash` can be passed.<br>• On the LDAP server: Allow already hashed passwords to be passed.<br>• In the synchronization project: Only pass hashed passwords. Use the script properties for mapping schema properties that contain passwords. Create the password's hash value in the script. | 29620 |
| Target system synchronization does not show any information in the Manager web application.<br>Workaround: Use Manager to run the target system synchronization. | 30271 |
| The following error occurs in One Identity Safeguard if you request access to an asset from the access request policy section and it is configured for asset-based session access of type **User Supplied**:<br>`400: Bad Request -- 60639: A valid account must be identified in the request.` | 796028, 30963 |

| Known Issue | Issue ID |
|---|---|
| The request is denied in One Identity Manager and the error in the request is displayed as the reason. | |
| The following error message is displayed while setting up a synchronization project for One Identity Safeguard:<br>`404: Not Found -- 0:`<br>Cause: An older One Identity Safeguard version that does not support One Identity Manager is in use.<br>Solution: Ensure that you are using One Identity Safeguard version 2.5. | 31048 |
| Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled.<br>Cause: The SharePoint connector loads all object properties into cache by default.<br>Solution:<br>• Correct the error in the target system.<br>- OR -<br>• 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`.<br>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 |

**Table 13: Identity and Access Governance**

| Known Issue | Issue ID |
|---|---|
| Moving a shelf to another shop and the recalculation tasks associated with it can block the DBQueue.<br>Solution:<br>Parent IT Shop nodes of shelves and shops cannot be changed once they have been saved.<br>***To move a product in a shelf to another shop***<br>• Select the task **Move to another shelf**.<br>- OR -<br>• Assign the product to a shelf in the new shop then remove the product | 31413 |

| Known Issue | Issue ID |
|---|---|
| assignment to the previous shelf.<br>Once you have moved all the products, you can delete the shelf. | |

**Table 14: Third party contributions**

| Known Issue | Issue ID |
|---|---|
| An error can occur during synchronization of SharePoint websites under SharePoint 2010. The method `SPWeb.FirstUniqueRoleDefinitionWeb()` triggers an `ArgumentException`. For more information, see https://support.microsoft.com/en-us/kb/2863929. | 24626 |
| Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting **File and Printer sharing** is not set on the server. This option is not set on domain controllers on the grounds of security. | 24784 |
| An error, TNS-12516, TNS-12519 or ORA-12520, sporadically occurs when connecting with an Oracle Database. Reconnecting normally solves this.<br>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.<br>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:<br>• Windows Server 2016: KB4462928<br>• Windows Server 2012 R2: KB4462926, KB4462921<br>• Windows Server 2008 R2: KB4462926<br>We do not know whether other Windows updates also cause this error.<br>The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory groups during provisioning and will be removed from future versions of One Identity Manager once Microsoft has resolved the problem. | 30575 |

| Known Issue | Issue ID |
|---|---|
| In certain circumstances, the wrong language is used in the Stimulsoft controls in the Report Editor. | 31155 |
| In the Manager web application, following errors can occur under Windows Server 2008 R2:<br>`System.Security.Cryptography.CryptographicException: Object was not found.`<br>`at System.Security.Cryptography.NCryptNative.CreatePersistedKey (SafeNCryptProviderHandle provider, String algorithm, String name, CngKeyCreationOptions options)`<br>Workaround:<br>1. In the Internet Information Services (IIS) Manager, select the application and then the **Advanced Settings** context menu item.<br>2. On the **Process Model** panel, set the option **Load User Profile** to **True**.<br>For more information, see https://support.microsoft.com/en-us/help/4014602. | 31995 |

# Schema changes

The following provides an overview of schema changes in One Identity Manager version 8.1 up to version 8.1.1.

## Target System Synchronization Module

- New column `DPRRootObjConnectionInfo.UID_QBMServerTag` for mapping the server function for distributing provisioning and single object synchronization processes over several servers.

## Target System Base Module

- Column `UNSAccountB.AccountName` extended from `nvarchar(64)` to `nvarchar(256)`.

## Oracle E-Business Suite Module

- New columns `XUserInserted`, `XUserUpdated`, `XDateInserted` and `XDateUpdated` in the `EBSUserInRespCompressed` table.

### SAP R/3 User Management Module

- New columns XUserInserted, XUserUpdated, XDateInserted and XDateUpdated in the HelperSAPUserInSAPRole table.
- New column SAPUserHasParameter.InheritInfo for mapping assignments origins.
- The column SAPUserHasParameter.ParameterValueDirect has been deleted.

### SAP R/3 Structural Profiles Add-on Module

- New columns XUserInserted, XUserUpdated, XDateInserted and XDateUpdated in the HelperSAPUserInSAPHRP table.

### Privileged Account Governance Module

- New column PAGReqPolicy.AllowLinkedAccountPwdAccess for inputting whether users can set password requirements for their linked accounts.
- New column PAGUsrGroup.UID_PAGIdentityProvider as reference to the authentication provider.
- New column PAGIdentityProvider.DomainNames as list of domains.
- New table PAGReqPolicyHasDirAccount for allocating more than one directory account for session access.
- The column PAGReqPolicy.UID_PAGDirAccountSessionAccess has been deleted.
- The column PAGUser.UID_PAGDirectory has been deleted.
- The column PAGUsrGroup.UID_PAGDirectory has been deleted.

### Identity Management Base Module

- New columns PersonWantsOrg.PeerGroupFactor and PersonWantsOrg.IsCrossFunctional to support peer group analysis for requests.
- New table QERWebAuthnKey for mapping Webauthn security keys.

### Attestation Module

- New columns AttestationCase.PeerGroupFactor and AttestationCase.IsCrossFunctional to support peer group analysis for attestation.
- New mandatory field definition for the column AttestationCase.UID_AttestationRun.

### Configuration Module

- New columns QBMBufferTransfer.OperationType and QBMModuleDef.CheckSumForDelta (in preparation of future functionality).

# Changes to system connectors

The following provides an overview of the modified synchronization templates and an overview of all patches supplied by One Identity Manager version 8.1 to version 8.1.1. Apply the patches to existing synchronization projects. For more information, see Applying patches to synchronization projects on page 57.

# 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 30.

**Table 15: Overview of synchronization templates and patches**

| Module | Synchronization template | Type of modification |
|---|---|---|
| Azure Active Directory Module | Azure Active Directory synchronization | changed |
| Active Directory Module | Active Directory synchronization | changed |
| Active Roles Module | Synchronize Active Directory domain via Active Roles | none |
| Cloud Systems Management Module | Universal Cloud Interface synchronization | none |
| Oracle E-Business Suite Module | Oracle E-Business Suite synchronization | changed |
| | Oracle E-Business Suite CRM data | none |
| | Oracle E-Business Suite HR data | changed |
| | Oracle E-Business Suite OIM data | none |
| Microsoft Exchange Module | Microsoft Exchange 2010 synchronization (deprecated) | changed |
| | Microsoft Exchange 2013/2016 synchronization (deprecated) | none |
| | Microsoft Exchange 2010 synchronization (v2) | changed |
| | Microsoft Exchange 2013/2016 synchronization (v2) renamed to: | changed |

| Module | Synchronization template | Type of modification |
|---|---|---|
| | Microsoft Exchange 2013/2016/2019 synchronization (v2) | |
| G Suite Module | G Suite synchronization | none |
| LDAP Module | AD LDS synchronization | none |
| | OpenDJ synchronization | none |
| IBM Notes Module | Lotus Domino synchronization | changed |
| Exchange Online Module | Exchange Online synchronization (deprecated) | none |
| | Exchange Online synchronization (v2) | changed |
| Privileged Account Governance Module | One Identity Safeguard synchronization | changed |
| SAP R/3 User Management Module | SAP R/3 Synchronization (Base Administration) | changed |
| | SAP R/3 (CUA subsystem) | none |
| SAP R/3 Analysis Authorizations Add-on Module | SAP R/3 BW | none |
| SAP R/3 Compliance Add-on Module | SAP R/3 authorization objects | none |
| SAP R/3 Structural Profiles Add-on Module | SAP R/3 HCM authentication objects | none |
| | SAP R/3 HCM employee objects | none |
| SharePoint Module | SharePoint synchronization | none |
| SharePoint Online Module | SharePoint Online synchronization | none |
| Universal Cloud Interface Module | SCIM Connect via One Identity Starling Connect | changed |
| | SCIM synchronization | changed |
| Unix Based Target Systems Module | Unix Account Management | 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 8.1.1. 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.

IMPORTANT: Some patches are applied automatically while One Identity Manager is updating. However, this only happens if you are updating a version of One Identity Manager that is older than One Identity Manager 8.1.

If you are updating an 8.1. version of One Identity Manager, you must apply patches manually.

For more information, see Applying patches to synchronization projects on page 57.

**Table 16: Patches for Azure Active Directory**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31456 | Make `User.CompanyName` writeable | Removes access restrictions for the `User.ComanyName` schema property. `CompanyName` can now be written to. | 31456 |

**Table 17: Patches for Active Directory**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31419 | Sets rule filters for various synchronization steps in the provisioning workflow | Sets blacklist rules for **group**, **domainDNS** and **builtinDomain** synchronization steps in the provisioning workflow.<br>This patch is applied automatically when One Identity Manager is updated. | 31419 |
| VPR#31792 | Object filter correction | Corrects object filters.<br>This patch is applied automatically when One Identity Manager is updated. | 31792 |

**Table 18: Patches for Microsoft Exchange**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31165 | Use local server date as revision | Creates new connection parameters and variables for the configuration of revision filtering. By default, the local server time is used for revision filtering. Therefore, the local server time and date are applied by default. | 31165 |
| VPR#30964 | Support | This patch ensures that, in the case of | 30964 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | for linked room mailboxes | `LinkedRoomMailboxes`, schema properties `LinkedCredential`, `LinkedDomainController` and `LinkedMasterAccount` are passed to the connector. | |

**Table 19: Patches for Exchange Online**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#30269 | Prevents errors when loading single objects due to identical display names | Changes the schema properties `vrtModBy`, `vrtAcceptMessagesFrom`, `vrtGrantSendOnBehalfOfTo`, `vrtRejectMessagesFrom` and all property mapping rules for these schema properties. | 30269 |
| VPR#31166 | Use local server date as revision | Creates new connection parameters and variables for the configuration of revision filtering. By default, the local server time is used for revision filtering. Therefore, the local server time and date are applied by default. | 31166 |

**Table 20: Patches for Oracle E-Business Suite**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31735 | Scope filter for schema type **PersonInLocality** | Creates a scope filter for schema type **PersonInLocality**.<br>This patch is applied automatically when One Identity Manager is updated. | 31735 |
| VPR#31782 | Security groups definition | Correction of security groups definition.<br>This patch is applied automatically when One Identity Manager is updated. | 31782 |
| VPR#31794 | Scope filter correction | Corrects scope filters.<br>This patch is applied automatically when One Identity Manager is updated. | 31794 |

**Table 21: Patches for IBM Notes**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31420 | Sets rule filters for various synchronization steps in the provisioning workflow | Sets blacklist rules for **Certifier** and **Policy** synchronization steps in the provisioning workflow.<br>This patch is applied automatically when One Identity Manager is updated. | 31420 |

**Table 22: Patches for Privileged Account Management**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31459 | Mapping der Schemaeigenschaft `AllowLinkedAccountPasswordAccess` | Adds a property mapping rule for the new `AllowLinkedAccountPasswordAccess` schema property to the `AccessRequestPolicy` mapping.<br>This patch is applied automatically when One Identity Manager is updated. | 31459 |
| VPR#31568A | Replaces **Appliance serial** as appliance identifier with a custom identifier (part 1) | Replaces **Appliance serial** as the unique identifier of the base object with a custom identifier and applies this change to the synchronization configuration.<br>Prerequisite for patch **Replaces Appliance serial as appliance identifier with a custom identifier (part 2)**<br>This patch is applied automatically when One Identity Manager is updated. | 31568 |
| VPR#31568B | Replaces **Appliance serial** as appliance identifier with a custom identifier (part 2) | Replaces **Appliance serial** as the unique identifier of the base object with a custom identifier and applies this change to the synchronization configuration.<br>Dependent upon patch **Replaces Appliance serial as appliance identifier with a custom identifier (part 1)**<br>This patch is applied automatically when One Identity Manager is updated. | 31568 |
| VPR#31569 | One Identity | Adds connection parameters and | 31569 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Safeguard cluster access improve-ments | variables for connecting One Identity Safeguard clusters.<br>This patch is applied automatically when One Identity Manager is updated.<br>If you use One Identity Safeguard clusters, run the system connection wizard after applying the patch, to determine the cluster's appliances. | |
| VPR#31664A | AccessRequestPolicy model changes for session access (part 1) | An access request policy can have multiple directory accounts for session access.<br>Prerequisite for patch **AccessRequestPolicy model changes for session access (part 2)**.<br>This patch is applied automatically when One Identity Manager is updated. | 31664 |
| VPR#31664B | AccessRequestPolicy model changes for session access (part 2) | An access request policy can have multiple directory accounts for session access.<br>Dependent on patch **AccessRequestPolicy model changes for session access (part 1)**.<br>This patch is applied automatically when One Identity Manager is updated. | 31664 |
| VPR#31703 | Additional rule for `Director` and `IdentityProvider` mappings | Adds an additional rule for the `Directory` and `Identityprovider` mappings.<br>This patch is applied automatically when One Identity Manager is updated. | 31703 |
| VPR#31775A | Change to user and user group references (part 1) | Removes the reference to the directory for users and user groups and adds a reference to the authentication provider for user groups.<br>Prerequisite for patch **Change to user and user group references (part 2)**.<br>This patch is applied automatically when One Identity Manager is updated. | 31775 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31775B | Change to user and user group references (part 2) | Removes the reference to the directory for users and user groups and adds a reference to the authentication provider for user groups.<br>Dependent on patch **Change to user and user group references (part 1)**.<br>This patch is applied automatically when One Identity Manager is updated. | 31775 |

**Table 23: Patches for SAP R/3**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31412 | Sets blacklist rules for provisioning | Sets blacklist property mapping rules in the `user` synchronization step of the provisioning workflow.<br>This patch is applied automatically when One Identity Manager is updated. | 31412 |
| VPR#31427 | Sets filter for `SAPUserInSAPRole` (XIsInEffect <> 0) | Creates schema class `AssignmentsInEffect` for schema type `SAPUserInSAPRole` with the filter `XIsInEffect <> '0'` and uses it in `userInRole` and `userInCUARole` mappings. | 31427 |
| VPR#31796 | Object filter correction | Corrects object filters.<br>This patch is applied automatically when One Identity Manager is updated. | 31796 |
| VPR#31930 | Change the reference scope for the schema type `SAPLicence` | Corrects the reference scope of the schema type `SAPLicence` in the One Identity Manager connection. | 31930 |

**Table 24: Patches for SharePoint Online**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31499 | Deletes `Site.NewUrl` schema property | Deletes `NewUrl` schema property from the `Site` mapping.<br>This patch is applied automatically when One Identity Manager is updated. | 31499 |

**Table 25: Patches for the SCIM interface (in Universal Cloud Interface Module)**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31733 | Schema properties with return type **request** | Updates the connector schema to handle schema properties with return type **request**.<br>This patch is applied automatically when One Identity Manager is updated. | 31733 |
| VPR#31756 | Access token scope | Creates a scope for the access token as a new connection parameter. | 31756 |

## Patches in One Identity Manager version 8.1

**Table 26: General patches**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **DPR**. | |
| | Milestone 8.1.1 | Milestone for the context **One Identity Manager**. | |

**Table 27: Patches for Azure Active Directory**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **Azure Active Directory**. | |

**Table 28: Patches for Active Directory**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#29087 | Add the schema property `mS-DS-ConsistencyGuid` | Adds the schema property `mS-DS-ConsistencyGuid` in the `User` and `InetOrgPerson` maps. | 29087 |
| VPR#29306 | Schema class `ADSSite (all)` (part 1) correction | Changes the foreign key for `ADSSite` from `ADSDomain` to `ADSFroest`.<br>Prerequisite for patch **Schema class ADSSite (all) (part 2) correction**.<br>This patch is applied automatically when One Identity Manager is | 29306 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | | updated. | |
| VPR#29306_2 | Schema class ADSSite (all) (part 2) correction | Changes the foreign key for ADSSite from ADSDomain to ADSFroest.<br>Dependent on patch **Schema class ADSSite (all) (part 2) correction**.<br>This patch is applied automatically when One Identity Manager is updated. | 29306 |
| VPR#30192 | Scope definition and usage of processing method MarkAsOutstanding | Adds a scope and the processing method MarkAsOutstanding to the synchronization step trustedDomain. | 30192 |
| | Milestone 8.1.1 | Milestone for the context **Active Directory**. | |

**Table 29: Patches for Active Roles**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#28612 | Adds new property mapping rules to the Computer mapping | Adds property mapping rules for OperatingSystem, OperatingSystemVersion and OperatingSystemServicePack to the Computer mapping. | 28612 |
| VPR#29087 | Add the schema property mS-DS-ConsistencyGuid | Adds the schema property mS-DS-ConsistencyGuid in the User and InetOrgPerson maps. | 29087 |
| | Milestone 8.1.1 | Milestone for the context **Active Roles**. | |

**Table 30: Patches for Oracle E-Business Suite**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#28962_EBS | Change date conversion in script properties | A language independent format is used for converting date values in script properties.<br>This patch is applied automatically when One Identity Manager is updated. | 28962 |
| VPR#29265 | Extended processing methods in the synchron- | Extended the synchronization configuration EBS_Person_ | 29265 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | ization step HR PersonManager | RemoveManager in the synchronization step HR PersonManager.<br>This patch is applied automatically when One Identity Manager is updated. | |
| VPR#29741 | Extended synchronization configuration by HR PersonPrimaryLocation | Extends a synchronization step and a mapping for synchronizing employees' primary locations. | 29741 |
| VPR#30464 | Support for Oracle Database Editions | Adds a variable to the Oracle Database Edition configuration. | 30464 |
| VPR#31011 | Change serialization format | Changes the serialization format of the schema types and reloaded the target system schema.<br>This patch is applied automatically when One Identity Manager is updated. | 31011 |
| | Milestone 8.1.1 | Milestone for the context **Oracle E-Business Suite**. | |

**Table 31: Patches for Microsoft Exchange**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#28815 | Extends a processing method in the synchronization step RoleAssignmentPolicy | Extends the processing method MarkAsOutstanding in the synchronization step RoleAssignmentPolicy. | 28815 |
| VPR#31026 | Optimizes revision filtering | Reloads the target system schema and replaces the revision counters whenChangedUTC and whenCreatedUTC with vrtRevision. | 31026 |
| | Milestone 8.1.1 | Milestone for the context **Microsoft Exchange**. | |

**Table 32: Patches for Exchange Online**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#30498 | Removes property mapping | Removes property mapping rules | 30498 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | rules from the `OwaMailboxPolicy` mapping | `BoxAttachmentsEnabled`, `DropboxAttachmentsEnabled` and `GoogleDriveAttachmentsEnabled` from the `OwaMailboxPolicy` mapping. | |
| VPR#30588 | Extends schema properties and property mapping rules in `Calendar Processing (User/Shared)` and `Calendar Processing (Resource)` mappings | Extends member lists in the schema properties `vrtBookInPolicy`, `vrtRequestInPolicy` and `vrtRequestOutOfPolicy` and updates the property mapping rules accordingly. | 30588 |
| VPR#31026 | Optimizes revision filtering | Reloads the target system schema and replaces the revision counters `whenChangedUTC` and `whenCreatedUTC` with `vrtRevision`. | 31026 |
| VPR#31269 | Modified implementation by extending various property mapping rules by a condition. | In the `Mailbox` mapping, a condition was added to various property mapping rules to modify implementation. | 31269 |
| | Milestone 8.1.1 | Milestone for the context **Exchange Online**. | |

**Table 33: Patches for G Suite**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **G Suite**. | |

**Table 34: Patches for LDAP**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **LDAP**. | |

**Table 35: Patches for IBM Notes**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#30313 | Mapping for mailbox file access levels | Inserts a property mapping rule for access levels of mailbox files in the `Person` mapping. | 30313 |
| | Milestone 8.1.1 | Milestone for the context **IBM Notes**. | |

**Table 36: Patches for SAP R/3**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#28147 | Deletes the mapping `userInMandant` | Deletes the mapping `userInMandant`. The map is replaced by `userMandant`.<br>Prerequisite for patch **New mapping `userMandant`**.<br>This patch is applied automatically when One Identity Manager is updated. | 28147 |
| VPR#28147_2 | New mapping `userMandant` | New mapping for accessing client user accounts (`userMandant`).<br>Depends on patch **Deletes the mapping `userInMandant`**.<br>This patch is applied automatically when One Identity Manager is updated. | 28147 |
| VPR#30453 | New property mapping rule for provisioning company data | New property mapping rule for mapping user account for provisioning company data.<br>This patch is applied automatically when One Identity Manager is updated. | 30453 |
| VPR#30941 | Sets blacklist rules for provisioning | Sets blacklist property mapping rules for the `userInCUARole` synchronization step of the provisioning workflow.<br>This patch is applied automatically when One Identity Manager is updated. | 30941 |
| | Milestone 8.1.1 | 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#29265 | Extends a processing method in the synchronization step `Managers` | Extended the processing method `SHR_Department_RemoveManager` in the synchronization step `Managers`<br>This patch is applied automatically when One Identity Manager is updated. | 29265 |
| | Milestone 8.1.1 | 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 8.1.1 | 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 |
|---|---|---|---|
| VPR#29477 | Applies the processing method `MarkAsOutstanding` | Applies the processing method `MarkAsOutstanding` in various synchronization step. | 29477 |
| | Milestone 8.1.1 | Milestone for the context **SAP R/3**. | |

**Table 40: Patches for SharePoint**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **SharePoint**. | |

**Table 41: Patches for SharePoint Online**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#30729 | Corrects the **Mandatory** property of the SharePoint Online `User.LoginName`. | Changes property **Mandatory** of schema property `LoginName` of schema class `User (all)`.<br>This patch is applied automatically when One Identity Manager is updated. | 30729 |
| | Milestone 8.1.1 | 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#30497 | Allows configuration of local cache | Adds a variable for disabling use of local cache.<br>This patch is applied automatically when One Identity Manager is updated. | 30497 |

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| VPR#31250 | Corrections to the scripts of virtual schema properties | Adds a NULL value test in the get scripts of virtual schema properties.<br>This patch is applied automatically when One Identity Manager is updated. | 31250 |
| | Milestone 8.1.1 | Milestone for the context **SCIM**. | |

**Table 43: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **Universal Cloud Interface**. | |

**Table 44: Patches for Unix**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **Unix**. | |

**Table 45: Patches for the One Identity Manager connector**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **Database**. | |

**Table 46: Patches for the CSV connector**

| Patch ID | Patch | Description | Issue ID |
|---|---|---|---|
| | Milestone 8.1.1 | Milestone for the context **CSV**. | |

# Deprecated features

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

- Oracle Database is no longer supported as a database system for the One Identity Manager database.

NOTE: Oracle Data Migrator is provided to help you convert the database system. The Oracle Data Migrator takes all the data belonging to an Oracle Database's database user from version 8.0.1 or later and transfers it to an SQL Server database with the same version.

You can obtain the tool and a quick guide from the support portal. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

- Google ReCAPTCHA Version 1 is no longer supported.
- The process component `SvnComponent` has been removed.
- The **Common | MailNotification | DefaultCultureFormat** configuration parameter has been deleted.

  Customized usage might require modification. The language for formatting values is determined through the current employee.
- The following scripts have been removed because their functions are obsolete or no longer ensured:
  - VI_Del_ADSAccountInADSGroup
  - VI_GetDNSHostNameOfHardware
  - VI_GetDomainsOfForest
  - VI_GetServerFromADSContainer
  - VI_Make_Ressource
  - VID_CreateDialogLogin
  - VI_Discard_Mapping
  - VI_Export_Mapping
  - VI_GenerateCheckList
  - VI_GenerateCheckListAll

The following functions are discontinued in future versions of One Identity Manager and should not used anymore.

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

  Use the Password Reset Portal to change passwords. Save your passwords and questions in the Web Portal.
- In future, the configuration parameter **QER | Person | UseCentralPassword | PermanentStore** will not be supported and will be deleted.
- In future, the table `OS` will not be supported and will be removed from the One Identity Manager schema.
- In future, the **viITShop** system user will not be supported and will be deleted.

  Use role-based login with the appropriate application roles.
- In future, the `VI_BuildPwdMessage` script will not be supported and will be deleted.

  Mail template are used to send email notifications with login information. The mail templates are entered in the **TargetSystem | ... | Accounts |**

**InitialRandomPassword | SendTo | MailTemplateAccountName** and **TargetSystem | ... | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameters.

# System requirements

Ensure that your system meets the following minimum hardware and system requirements before installing One Identity Manager. For more detailed information about system prerequisites, see the *One Identity Manager Installation Guide*.

# Minimum requirements for the database server

| | |
|---|---|
| Processor | 8 physical cores 2.5 GHz+<br>NOTE: 16 physical cores are recommended on the grounds of performance. |
| Memory | 16 GB+ RAM |
| Hard drive storage | 100 GB |
| Operating system | Windows operating system<br>• Note the requirements from Microsoft for the SQL Server version installed.<br>UNIX and Linux operating systems<br>• Note the minimum requirements given by the operating system manufacturer for SQL Server databases. |
| Software | Following versions are supported:<br>• SQL Server 2017 Standard Edition (64-bit) with the current cumulative update<br>• SQL Server 2016 Standard Edition (64-bit), Service Pack 2 with the current cumulative update<br>• Compatibility level for databases: SQL Server 2016 (130)<br>• Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended)<br>NOTE: The SQL Server Enterprise Edition is strongly recommended on performance grounds. |

# Minimum requirements for the service server

| | |
|---|---|
| Processor | 8 physical cores 2.5 GHz+ |
| Memory | 16 GB RAM |
| Hard drive storage | 40 GB |
| Operating system | Windows operating system<br>Following versions are supported:<br>• Windows Server 2019<br>• Windows Server 2016<br>• Windows Server 2012 R2<br>• Windows Server 2012<br>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later<br>Linux operating system<br>• Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. |
| Additional software | Windows operating system<br>• Microsoft .NET Framework Version 4.7.2 or later<br>NOTE: Take the target system manufacturer's recommendations for connecting the target system into account.<br>Linux operating system<br>• Mono 5.14 or later |

# Minimum requirements for clients

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

| | |
|---|---|
| | • Windows 10 (32-bit or 64-bit) with version 1511 or later<br>• Windows 8.1 (32-bit or 64-bit) with the current service pack<br>• Windows 7 (32-bit or non-Itanium 64-bit) with the current service pack |
| Additional software | • Microsoft .NET Framework Version 4.7.2 or later |
| Supported browsers | • Internet Explorer 11 or later<br>• Firefox (Release Channel)<br>• Chrome (Release Channel)<br>• Microsoft Edge (Release Channel) |

# Minimum requirements for the Web Server

| | |
|---|---|
| Processor | 4 physical cores 1.65 GHz+ |
| Memory | 4 GB RAM |
| Hard drive storage | 40 GB |
| Operating system | Windows operating system<br>• Windows Server 2019<br>• Windows Server 2016<br>• Windows Server 2012 R2<br>• Windows Server 2012<br>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later<br>Linux operating system<br>• Linux operating system (64-bit), supported by the Mono project or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server. |
| Additional software | Windows operating system<br>• Microsoft .NET Framework Version 4.7.2 or later<br>• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and Role Services:<br>  • Web Server \| Common HTTP Features \| Static Content<br>  • Web Server \| Common HTTP Features \| Default Document |

- Web Server | Application Development | ASP.NET
- Web Server | Application Development | .NET Extensibility
- Web Server | Application Development | ISAPI Extensions
- Web Server | Application Development | ISAPI Filters
- Web Server | Security | Basic Authentication
- Web Server | Security | Windows Authentication
- Web Server | Performance | Static Content Compression
- Web Server | Performance | Dynamic Content Compression

Linux operating system

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

# Minimum requirements for the Application Server

| | |
|---|---|
| Processor | 8 physical cores 2.5 GHz+ |
| Memory | 8 GB RAM |
| Hard drive storage | 40 GB |
| Operating system | Windows operating system<br>• Windows Server 2019<br>• Windows Server 2016<br>• Windows Server 2012 R2<br>• Windows Server 2012<br>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later<br>Linux operating system<br>• Linux operating system (64-bit), supported by the Mono project or |

| | |
|---|---|
| | Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server. |
| Additional software | Windows operating system<br>• Microsoft .NET Framework Version 4.7.2 or later<br>• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and Role Services:<br>  • Web Server \| Common HTTP Features \| Static Content<br>  • Web Server \| Common HTTP Features \| Default Document<br>  • Web Server \| Application Development \| ASP.NET<br>  • Web Server \| Application Development \| .NET Extensibility<br>  • Web Server \| Application Development \| ISAPI Extensions<br>  • Web Server \| Application Development \| ISAPI Filters<br>  • Web Server \| Security \| Basic Authentication<br>  • Web Server \| Security \| Windows Authentication<br>  • Web Server \| Performance \| Static Content Compression<br>  • Web Server \| Performance \| Dynamic Content Compression<br>Linux operating system<br>• NTP - Client<br>• Mono 5.14 or later<br>• Apache HTTP Server 2.0 or 2.2 with the following modules:<br>  • mod_mono<br>  • rewrite<br>  • 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 | Any delimited text files. |

| Connector | Supported data systems |
|---|---|
| text files | |
| Connector for relational databases | Any relational databases supporting ADO.NET.<br>NOTE: Additional installation of an ADO.NET data provider from a third party may be necessary. Ask Microsoft or the relational database producer. |
| Generic LDAP connector | Any LDAP directory server conforming to version 3. The LDAP connector requires the directory server to be RFC conform. Specifically, to conform to the standards RFC 4514 (String Representation of Distinguished Names) and RFC 4512 (Directory Information Models).<br>NOTE: Other schema and provisioning process adjustments can be made depending on the schema. |
| Web service connector | Any SOAP web service providing wsdl.<br>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 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016. |
| Microsoft Exchange connector | • Microsoft Exchange 2010 Service Pack 3 or later<br>• Microsoft Exchange 2013 Service Pack 1 or later<br>• Microsoft Exchange 2016<br>• Microsoft Exchange 2019 with cumulative update 1<br>• Microsoft Exchange hybrid |
| SharePoint connector | • SharePoint 2010<br>• SharePoint 2013<br>• SharePoint 2016<br>• SharePoint 2019 |
| SAP R/3 connector | • SAP Web Application Server 6.40<br>• SAP NetWeaver Application Server 7.00, 7.01, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2 and 7.50<br>• SAP ECC 5.0 and 6.0<br>• SAP S/4HANA On-Premise-Edition |
| Unix | Supports the most common Unix and Linux derivatives. For more |

| Connector | Supported data systems |
|---|---|
| connector | information, see the Authentication Services specifications. |
| IBM Notes connector | • Lotus Domino Server Version 8.0 up to Lotus Domino Server Version 9.0<br>• IBM Notes Client 8.5.3 is supported as client version. |
| Native database connector | • SQL Server<br>• Oracle Database<br>• SQLite<br>• MySQL<br>• DB2 (LUW)<br>• CData ADO.NET Provider<br>• SAP HANA |
| Mainframe connector | • RACF<br>• IBM i<br>• CA Top Secret<br>• CA ACF2 |
| Windows PowerShell connector | • Windows PowerShell version 3 or later |
| Active Roles connector | • Active Roles 6.9, 7.0, 7.2, 7.3.1 |
| Azure Active Directory connector | • Microsoft Azure Active Directory |
| SCIM connector | Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0. |
| Exchange Online connector | • Microsoft Exchange Online |
| G Suite Connector | • G Suite |
| Oracle E-Business Suite connector | • Oracle E-Business Suite System versions 12.1 and 12.2 |

| Connector | Supported data systems |
|---|---|
| SharePoint Online connector | • Microsoft SharePoint Online |
| One Identity Safeguard connector | • One Identity Safeguard versions 2.5, 2.6, 2.7 |

# Product licensing

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

# Upgrade and installation instructions

To install One Identity Manager 8.1.1 for the first time, follow the installation instructions in the *One Identity Manager Installation Guide*. For more detailed instructions about updating, see the *One Identity Manager Installation Guide*.

IMPORTANT: Note the Advice for updating One Identity Manager on page 51.

# Advice for updating One Identity Manager

- Ensure that the administrative system user, who is going to compile the database, has a password before you update the One Identity Manager database to version 8.1.1. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
  - Automatic software updating of version 7.0 to version 8.1.1 only works smoothly if the service pack 7.0.3 is installed. In addition, the files `VI.Update.dll` and `JobService.dll` must be installed.

    Request the files `VI.Update.dll` and `JobService.dll` from the support portal.

    To distribute the file, use the Software Loader.

    Future service packs of 7.0 versions will already contain the changes to these files, and therefore, must not distributed separately.

    - Automatic software updating of version 7.1 to version 8.1.1 only works smoothly if the service pack 7.1.3 is installed.
- 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. Ensure that the user that going to execute the installation or update of the One Identity Manager database, owns the **dbcreator** SQL Server server role.
- During the update of a One Identity Manager database version 7.0, 7.1 or 8.0 to version 8.1.1, 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\Files\MSSQL2K\30374.sql`) is provided. In case it fails, correct the data and restart the update.
- During installation of a new One Identity Manager database or a new One Identity Manager History Database with version 8.1.1 or while updating an One Identity Manager database or One Identity Manager History Database from version 7.0.x, 7.1.x or 8.0.x to version 8.1.1, 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*.

  Adjust the configuration parameter after updating the One Identity Manager. 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.

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

- To successfully compile HTML applications with the Configuration Wizard, you must download packages from the NPM repository. Ensure that the workstation running the Configuration Wizard can establish a connection to the website https://registry.npmjs.org.

  Alternatively, it is possible to download the packages from a proxy server and make them available manually. For more information, see the knowledge article https://support.oneidentity.com/kb/266000.

- In One Identity Manager versions 8.0, 8.0.1, 8.0.2, the One Identity Manager History Service and the One Identity Manager Service were both installed when the One Identity Manager History Database was installed.

  If you are affected by this problem, uninstall the One Identity Manager History Service before updating your One Identity Manager History Database. Run the following command as administrator:

  ```
  sc delete "HDBService"
  ```

# Updating One Identity Manager to version 8.1.1

IMPORTANT: Note the Advice for updating One Identity Manager on page 51.

***To update an existing One Identity Manager installation to version 8.1.1***

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

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

NOTE: To update a One Identity Manager History Database installation, change to the **Other Products** page and select the **One Identity Manager History Database**.

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. (From version 7.0.x or version 7.1.x) End the One Identity Manager Service on the server that processes direct database queries.

   (From version 8.0.x or version 8.1.x). End 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 to **130** and change the value if required.
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 7.0.x, 7.1.x or 8.0.x to version 8.1.1, 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 to version 8.1.1, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

7. (From version 7.0.x or version 7.1.x) Update the One Identity Manager Service on the server that processes direct database queries.

(From version 8.0.x or version 8.1.x). Update the One Identity Manager Service on the update server.

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

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

> NOTE: To update a One Identity Manager History Database installation, change to the **Other Products** page and select the **One Identity Manager History Database**.

c. Click **Install**.

This starts the installation wizard.

d. Follow the installation instructions.

> IMPORTANT: Select the directory you used for your previous installation as the installation directory on the **Installation settings** page. 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. Revert to the original settings if the One Identity Manager Service did not initially use the local system account for logging in. Specify the service account to be used. Enter the service account to use.
9. Start the One Identity Manager Service on the update server.
10. Update other installations on workstations and servers.

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

### *To update synchronization projects to version 8.1.1*

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 execute the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

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

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

For more information, see Applying patches to synchronization projects on page 57.

***To update an application server to version 8.1.1***

- 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 Portal to version 8.1.1***

NOTE: Ensure that the application server is updated before you install the Web Portal. As from version 7.1. and later, the Web Portal requires an application server with a search service installed on it.

- To update the 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 Portal, uninstall the existing Web Portal and install the Web Portal again. For more information, see the *One Identity Manager Installation Guide*.

***To update an API Server to version 8.1.1***

- 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 8.1.1***

- (As from version 8.1.x) After updating the API Server, compile the HTML application **Operations Support Portal**. For more information, see the *One Identity Manager Installation Guide*.
- (As from version 8.0.x)
  1. Uninstall the Operations Support Web Portal.
  2. Install an API Server and compile the HTML application **Operations Support Portal**. For more information, see the *One Identity Manager Installation Guide*.

***To update the Manager web application to version 8.1.1***

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 change customizations in synchronization projects. This mean that conflicts may occur if patches are applied to synchronization projects, which have been customized. This may cause loss of data.**

***Before you apply a patch***

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

NOTE: If you 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. Open the synchronization project in the Synchronization Editor.
2. Select **Edit | Update synchronization project...** from the menu.
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. 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 more detailed information about updating synchronization projects, see the *One Identity Manager Target System Synchronization Reference Guide*.

See also:

- Modified synchronization templates on page 29
- Patches for synchronization projects on page 30

# Verifying successful installation

***To determine if this version is installed***

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

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

  The version number 2019.0001.0021.0100 for all modules and the application version 8.1 2019-01-21-108 indicate that this service pack is installed.

# Additional resources

Additional information is available from the following:

- One Identity Manager support
- One Identity Manager online documentation
- Identity and Access Management community
- One Identity Manager training portal

# 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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

# Technical support resources

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

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

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

**Legend**

**WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.