

# One Identity Manager 8.0.5

## Release Notes

### May 2020

These release notes provide information about the One Identity Manager release. You will find all the modifications since One Identity Manager version 8.0.4 listed here.

One Identity Manager 8.0.5 is a patch release with enhanced features and functionality. See [Enhancements](#) on page 2.

If you are updating a One Identity Manager version prior to One Identity Manager 8.0.4, 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](#).

For changes to the Web Designer and the Web Portal since the last version, see the document *Web Designer and Web Portal Changes*.

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

# About One Identity Manager 8.0.5

One Identity Manager simplifies the process of managing user identities, access permissions and security policies. You allow the company control over identity management and access decisions whilst the IT team can 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.

## Enhancements

The following is a list of enhancements implemented in One Identity Manager 8.0.5.

**Table 1: General**

Enhancement	Issue ID
Improved performance updating the current UTC time difference of all timezones.	32567
New parameters of the ScriptComponent process component are available for the CSVExport and CSVExportSingle process tasks. <ul style="list-style-type: none"><li>• ValueMaskChar: Character for masking values. If the parameter exists, the character is automatically added at both ends of each value and every time the same character appears within the value, it is doubled.</li><li>• Culture: Language to use for formatting the value.</li><li>• ConvertUtcTimes: Specifies whether UTC times are converted to local times.</li><li>• TimeZone: For converting to the timezone to use. Only used if the ConvertUtcTimes is set. If the parameter is not set, the Job server's local timezone is used.</li></ul>	32410, 32939
Improved the <b>Objectkey references to non existing object</b> consistency check.	32333

**Table 2: General web applications**

<b>Enhancement</b>	<b>Issue ID</b>
In the Web Portal, the system role's Hyper View has been reworked.	20188
Improved performance requesting products in the Web Portal.	32255
Improved performance of certain database queries in the Web Portal.	32253
In the Web Portal, keyboard shortcuts are now displayed for all buttons (for example, <b>[Alt-C]</b> ).	31882
Improved performance of database-bound grids.	32393

**Table 3: Target system connection**

<b>Enhancement</b>	<b>Issue ID</b>
Improved performance provisioning assignments of Oracle E-Business Suite entitlements to user accounts.	32498
The SCIM connector now uses the service provider's default value to find the maximum number of objects per page. The connector does not send values anymore.	32684
Improved messages for the SCIM connector in the synchronization log.	32689, 32690
Improved performance determining employees that are responsible for a target system groups.	32855
Improved performance provisioning G Suite user accounts.	32884
The filter for the HRPerson_0709_IDEXT schema class was changed from a string to an integer comparison. A patch with the patch ID VPR#32899 is available for synchronization projects.	32899
The recommendations from Microsoft about avoiding throttling during SharePoint Online synchronization have been implemented.	32929
Improved documentation of permissions required for integrating One Identity Manager as an application in Azure Active Directory.	32820

**Table 4: Identity and Access Governance**

<b>Enhancement</b>	<b>Issue ID</b>
Improved performance creating and by approval of attestation cases.	32940
Improved performance calculating QER_FTPW0VisibleForPerson.	32334

Enhancement	Issue ID
Improved indexing of the PersonHasObject and BaseTreeHasObject tables.	32771
The <b>Retain service item assignment on relocation</b> option can now be set on default service items.	32588
In the Manager, on the overview forms for application roles, departments, cost centers, location and business roles, you can now see which approval workflows they are used in.	32745

See also:

- [Schema changes](#) on page 23
- [Patches for synchronization projects](#) on page 25

## Resolved issues

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

**Table 5: General**

Resolved issue	Issue ID
Custom files are deleted during update installation of local assemblies.	28985
Tests for possibly damaging SQL statements are too strict.	32102, 32285
Error, if the name of the connection server for transferring data to the One Identity Manager History Database contains special characters.	32163
When a connection server is created, data transfer to a One Identity Manager History Database fails if the <b>is_rpc_out_enabled</b> option is not set.	32492
Transaction scope of the DBQueue Processor's HDB-K-ProcessGroup task is too big.	32761
In certain circumstances, not all elements are indexed in the search index.	31881
In the search index, the change date is set even though a table is not indexed in a run.	32406
In certain circumstances, table relations are incorrectly identified as errors in the consistency check.	32443
The <b>_Old</b> suffix causes errors during bulk updating of column names.	32488
Internal temporary table for determining historical data for reports is created	32555

<b>Resolved issue</b>	<b>Issue ID</b>
with the wrong sort order.	
In certain circumstances, an error occurs in the QBM_PDBQueueProcess_De1 procedure.	32332
Blocked slots are reset too frequently.	32585
In certain circumstances in the DBTransporterCMD.exe command line program, single user mode is not exited.	32620
Insufficient references in certain scripts.	32644
An error occurs in a date field if the value larger than <b>31.12.9998</b> is entered.	32368
Incorrect sorting of date values in the Manager if <b>English (USA)</b> is set as the language.	32441
ObjectWalker does not work with dynamic foreign keys in a Data Import script.	32214
Input of dates in reports does not support every date format.	32775
When a report is translated, the description is not translated.	32875
Processes are sporadically not generated from schedules.	32742
The <b>Table with XOrigin (XIsInEffect) without update handling</b> consistency check does not take automatically generated triggers into account.	32902
Results of a SQL query in the Object Browser cannot be marked with <b>Ctrl + A</b> anymore.	32942
If the time difference to UTC for a timezone changes, the mean time difference to UTC for the states in this timezone is not updated.	32973
Export definitions for data export are not saved in the user configuration and are therefore not available after the Manager has been restarted.	32887

**Table 6: General web applications**

<b>Resolved issue</b>	<b>Issue ID</b>
Information about the password strength is not displayed in the respective language in the Password Reset Portal.	30694
In the Web Portal, you can sort by columns with hidden content.	31969
In the Web Portal, the <b>Back</b> button on the <b>Pending attestations</b> page only works if there are no attestations.	31963
In the Web Portal, on the <b>Pending attestations</b> page, an error occurs when you click the <b>Business roles</b> tile.	32920

Resolved issue	Issue ID
If an auditor in the Web Portal searches through requests ( <b>Requests   Auditing   Request</b> ), not all the results are found.	32069
In the Web Portal, selecting an employee for a new request can take a long time.	32372
In certain circumstances, an error occurs if you try to display a request template in the Web Portal.	32819
An error occurs when an approver in the Web Portal adds an item to another employee's request and sends the request.	32880
In the Web Portal, an error occurs if an empty grouped table is exported as a PDF.	32773
In the Web Portal, if you download a file with Internet Explorer 11 whose name contains non-ASCII characters, an incorrect file name is suggested for the file.	32921
If an error alert is displayed in the Web Portal and you try to close it using the <b>Escape</b> key, the underlying dialog is closed instead of just the error alert.	33020
In the Web Portal, an error occurs if a product request is displayed that is not assigned to an IT Shop.	32837
In the Web Portal, if a direct assignment of an SAP role to an SAP user account is removed, the associated entry in SAPUserInSAPRole is not deleted.	32842
In the Web Portal, requests to be approved can be selected in a list. In certain circumstances, the selection goes missing when you swap to the other side of the list.	32904
Use of the   character in the password of the SQL user who is used to install a web application causes an error.	32461
In the Web Designer, an error occurs if a project is compiled that contains a combobox node that is not iterated.	32366
In the Web Designer, some Web SQL functions cannot be used in conditions in column lists.	32374
The Web Designer's GetDataState function does not work and returns a value of <b>false</b> even if columns have changed.	32790
Bad performance of the pre-defined Webportal.VI_ITShop_ProductSelection.AccProductStatusForPerson SQL statement.	32767
In Web Designer, if you add a column of XdateInserted or XdateUpdated type to a table, the filter function for the column does not work in the Web Portal.	32709
In the Manager web application, an error occurs displaying rule violations.	32304
In the Web Designer, memory usage increases when working on module extensions.	32900

**Table 7: Target system connection**

<b>Resolved issue</b>	<b>Issue ID</b>
In the synchronization log, objects that are marked as outstanding are not logged.	32011
Objects with a combined primary key with a value of timestamp cannot be reloaded.	32266
The native database connector executes the configured processing method of a synchronization step only for the first object of the object class although several objects need to be processed. This happens if a pattern-based strategy is defined for the data operation.	32307
When you close a synchronization project, the password for logging in to the target system is saved incorrectly if it contains the dollar (\$) character.	32226, 32311
Error updating the schema from a CSV file if the file has not been declared in the system connection wizard.	32391
Special characters are not masked correctly in custom project templates.	32474
Error during synchronization: The connection does not support MultipleActiveResultSets.	32604
The IsSecret and IsSystemVariable properties of the DefaultUserPassword variable are not all correctly set in the synchronization project. Patches with patch IDs VPR#32781_SCIM, VPR#32781_EBS, VPR#32781_NDO are available for synchronization projects.	32781
Error adding memberships in the UNSAccountBInUNSGroupB table in the target system browser although the object are within the scope.	32532
Error testing the connection to the cloud application in the system connection wizards if there is no authentication endpoint given.	32627
If an error occurs loading the object list, the SCIM connector returns an empty list as successfully loaded. The error only occurs in One Identity Manager version 7.1.x and 8.0.x.	32646
Error serializing complex properties from schema extensions in synchronization projects with the SCIM connector.	32696
The SCIM connector uses the wrong media type for POST queries in the HTTP header. The data are swapped around.	32712
The provisioning process for a cloud application's user accounts returns the wrong data for loading the objects.	32780
Error provisioning group memberships if the SCIM connector uses PATCH queries.	32846

<b>Resolved issue</b>	<b>Issue ID</b>
Provisioning of deleted group memberships does not work under certain conditions.	32853
Changes to values of multi-valued schema properties are not correctly mapped in PUT queries.	32901
The User.address~primary schema property is set to <b>True</b> even if no address data is given. A patch with the patch ID VPR#32754 is available for synchronization projects.	32754
If a container is deleted from an Active Directory user account, verification of the object properties fails after provisioning. A patch with the patch ID VPR#32258 is available for synchronization projects.	32258
If an Active Directory object that already has the SAMAccountName exists in another container in Active Directory, an error occurs.	32504
Error during synchronization if accessing special properties of Active Directory objects using a DirectoryEntry object's extension method.	32873
Active Directory account policies that are assigned through Active Directory groups are not taken into account doe Active Directory user accounts.	32803
In the Manager, some assignment forms for Active Directory objects can be opened with multi-select.	32438
In the Manager, the <b>Change master data</b> form ( <b>FormADSAccountMasterData</b> ) does not show changes to the <b>Dial-up permitted</b> property for Active Directory user accounts (ADSAccount.AllowDialI).	32889
The Active Roles connector does not support the function level for Windows Server 2016 domains. A patch with the patch ID VPR#32844 is available for synchronization projects.	32844
The edsawTSUserConfigInheritInitialProgram property in the User mapping is negated. This behavior is no longer required. A patch with the patch ID VPR#32871 is available for synchronization projects.	32871
Problems connecting to Microsoft Exchange Server 2016 if using SSL.	32362
The ThrottlingPolicy property is not loaded for Microsoft Exchange mailboxes.	32533
The Notes connector returns the wrong value for AdminRequest.Type.	32589
Error provisioning Notes user accounts if the user account's certificate has been changed.	32705
The process for locking Notes user accounts does not work correctly.	32947



Resolved issue	Issue ID
The system connection to SAP R/3 cannot be established if the synchronization user's password contains dollar (\$) characters.	32298
Parameters used to call a BAPI function to delete an SAP object are incorrectly populated.	32469
SAPTitle.DistinguishedName is not unique. SAPTitle.DistinguishedName and SAPTitle.CanonicalName have been extended by the language code of the title. This makes the entries unique, even if several languages are maintained in the SAP system. A patch with the patch ID VPR#32584 is available for synchronization projects.	32584
If SAP user accounts marked for deletion are reset, the associated SAPUser-InSAPRole entries remain marked for deletion and are not reset.	32727
The IsSecret and IsSystemVariable properties of the TempUserPassword variable are not all correctly set in the synchronization project. A patch with the patch ID VPR#32781_SAP is available for synchronization projects.	32781
If Oracle E-Business Suite editions are used, the Oracle E-Business Suite connector accesses the wrong data sets. A patch with the patch ID VPR#30464 is available for synchronization projects.	30464
During synchronization, an invalid entitlement assignment is not re-enabled if it exists in Oracle E-Business Suite as a valid assignment. EBSUser-InResp.XOrigin retains the value <b>16</b> .	33024
When assigning account definitions to employees, process steps are not handled correctly anymore afterward. The status of the process step, to test whether a user account exists, is not set correctly in the JobQueue. The user account is created anyway. Subsequent processing of downstream tasks is blocked for the affected employee.	32580
On the form for defining search criteria for employee assignment, the allocated base object's UID is display instead of the user account's UID. This happens if the display pattern for the user account table is made up of several columns.	32612
On the form for defining search criteria for employee assignment, employees' display names are not correctly formatted.	32876
In the Manager, custom columns of Datetime type are not displayed with the desired alternative column identifier for custom target systems.	32702
Checking for the existence of target system objects fails if there are several mappings.	32908

**Table 8: Identity and Access Governance**

<b>Resolved issue</b>	<b>Issue ID</b>
If E-Business Suite permissions assignments to user accounts are attested and automatic removal of permissions is configured, denied assignments are not deleted.	30375
The condition for viewing the AttestationCase table of the <b>VI_4_ALLUSER</b> permissions group does not allow closed attestation cases to be displayed if the currently logged in user was involved.	31365
Automatic removal of permissions after attestation is denied does not taken into account whether the assignment is already marked for deletion or not.	32661
Notifications from questions about an attestation case are sent to the wrong employee.	32809
Error adding attestation cases.	32988
Error automatically removing E-Business Suite entitlement assignments after attestation has been denied.	32961
After the second step in an attestation case approval workflow, no more mail notifications are sent.	33049
In certain circumstances, an employee can make an approval decision for a request that was questioned.	32465
If an additional approver was assigned to an approval step, the chief approval team's approval decision has no effect.	32467
The QER_ZITShopOrderAbort procedure uses the wrong cancellation method.	32522
If an approver makes approval decisions for several requests because they are delegated, the delegator is only informed the first time.	32526
In certain circumstances, despite the <b>QER   ITShop   DeleteClosed</b> configuration parameter being set, not all columns that are marked to be logged on deletion are logged.	32559
The consistency check's repair script <b>Requested products that are not assigned</b> generates missing entries in the PersonInITShopOrg table with the wrong value for XOrigin.	32827
Under certain circumstances, when determining a request's approver, a fallback approver is not found although there is no regular approver.	32872
The <b>Replace</b> method is not available for requests with Renewal status.	33029
In certain reports about employees, the time period for assignments is not calculated correctly.	31955
Performance problems calculating system role assignment to business roles	32546

<b>Resolved issue</b>	<b>Issue ID</b>
and organizations.	
In the Manager, employees are shown on the <b>Subscribable report overview</b> form that do not subscribe to that report anymore.	32473
If a simple report is generated in CSV format, Display values about FK relations are not displayed properly.	32547
In certain reports about employees, the time period for assignments is not calculated correctly.	32389
Error calculating time periods for memberships in reports with historical data.	32726
The GenProcID in requests is emptied too quickly if an approved request's validity period is in the future.	32720
If, in the permissions editor for SAP functions, the <b>Add by</b> task is run and One Identity Manager is running over an application server, the Manager freezes.	32789

**Table 9: IT Service Management**

<b>Resolved issue</b>	<b>Issue ID</b>
In the Manager, the <b>Help desk employee</b> option on an employee's master data form, is not displayed correctly if you swap between employees.	32587
In the Manager, diverse master data are missing on the PC and server master data forms.	32922

See also:

- [Schema changes](#) on page 23
- [Patches for synchronization projects](#) on page 25

## 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**

<b>Known Issue</b>	<b>Issue ID</b>
If you connect to a database with the Database Compiler, the task QBM-K-	23049,

Known Issue	Issue ID
CommonWaitForCompiler is immediately queued in the DBQueue. If Database Compiler ends without compiling the database, the task remains in the DBQueue.	24713
Error in the Report Editor if columns are used that are defined in the Report Editor as keywords.  Workaround: Create the data query as 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
Header text in reports saved as CSV are not given their correct names.	24657
Number of ParamName/ParamValue parameter pairs in the MailComponent's SendRichMail process task is not always sufficient.  10 parameter pairs are available by default. If this number is not sufficient, you can add additional custom process parameters, which Process Editor can then use as parameters. This function is available as from One Identity Manager version 7.0.	25164
In certain circumstances, objects can be in an inconsistent state after simulation in the Manager. If an object is changed or saved during simulation and the simulation is finished, the object remains in the final simulated state. It may not be possible to save other modifications to this object instance.  Solution: Reload the object after completing simulation.	12753
Invalid module combinations can be selected in the Configuration Wizard. This causes errors at the start of the schema installation.  Cause: The Configuration Wizard was started directly.  Solution: Always use autorun.exe for installing One Identity Manager components. This ensures that you do not select any invalid modules.	25315
Schema extensions on a database view of type <b>View</b> (for example, Department) with a foreign key relation to a base table column (for example, BaseTree) or a database view of type <b>View</b> are not permitted.	27203
Error connecting through an application server if the certificate's private key, used by the VI.DB to try and encrypt its session data, cannot be exported and the private key is therefore not available to the VI.DB.  Solution: Mark the private key as exportable if exporting or importing the certificate.	27793
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	28373

Known Issue	Issue ID
database cannot be compiled.	
<p>Error resolving events on a view that does not have a UID column as a primary key.</p> <p>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 a rudimentary basic functionality in the system.</p> <p>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.</p> <p>The consistency check <b>Table of type U or R with wrong PK definition</b> is provided for testing the schema.</p>	29535
<p>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.</p>	30048
<p>The One Identity Manager Service only logs messages in the event log <b>Application</b>, by default.</p> <p>Cause: To add an event log with another name, you require administrator permissions on the Job server.</p> <p>Solution:</p> <ol style="list-style-type: none"> <li>1. Add the file that the One Identity Manager Service should write to manually on the Job server. You can use Windows PowerShell, for example, to do this. <ol style="list-style-type: none"> <li>a. Run Windows PowerShell as administrator on the Job server.</li> <li>b. Run the following CmdLet: <pre>New-EventLog -Source "Foobar" -LogName "&lt;file name&gt;"</pre> </li> </ol> </li> <li>2. Enter this file name in the One Identity Manager Service's configuration file as the name for the event log in the module Logwriter .</li> <li>3. Restart the computer.</li> <li>4. Restart the One Identity Manager Service.</li> </ol>	30540
<p>The configuration parameter <b>QER   ITShop   LimitOfNodeCheck</b> specifies how many product nodes are deleted in one DBQueue Processor run if large numbers of products in the IT Shop are deleted through automatic processes. By default, 500 objects are processed in one run. Set the value lower if there are performance problems while executing the task QER-K-OrgAutoChild.</p>	30657
<p>Outstanding objects are ignored by inheritance calculation. This means, all memberships and assignments remain intact until the outstanding objects</p>	30909

**Known Issue****Issue ID**

have been processed.

Start target system synchronization to do this.

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. 30972

The error, in case a Save Transaction is carried out is: Cannot use SAVE TRANSACTION within a distributed transaction.

Solution: Disable the option `DTC_SUPPORT = PER_DB`.

**Read Only** type tables with Common Table Expressions (CTE) in the ViewAddOn are not added in the schema.

As from One Identity Manager 7.0, the behavior of CTEs with the `with` keyword as condition for view definitions in database views of **Read only** type has changed. The conditions for view definitions are embedded in a summary query. This means, you cannot be sure that a common table expression is the very first expression in a query.

Possible error message:

```
(execute slot single)50000 0 re-throw in Procedure QBM_ZViewBuildR, Line 1050000 0 rethrow in Procedure QBM_PViewBuildR_intern, Line 10250000 0 re-throw in Procedure QBM_PViewBuildR_intern, Line 8250000 0 re-throw in Procedure QBM_PViewBuild_FromAddOn, Line 6550000 0 re-throw in Procedure QBM_PSQLCreate, Line 26156 0 detected in (...) Procedure ..., Line 6156 0 Incorrect syntax near the keyword 'with'
```

Recommended action:

1. Create a database view using Common Table Expressions.

Example:

```
create view CCC_Vxy as
with myWithClause (column1, column2) as (
select 1 as column1, 2 as column2
)
select * from myWithClause
go
```

2. Use the database view in the additional view definition (QBMViewAddon) of **Read only** type database views.

```
select * from CCC_Vxy
```

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.

31322

**Table 11: General web applications**

Known Issue	Issue ID
<p>The error message This access control list is not in canonical form and therefore cannot be modified sometimes occurs when installing the Web Portal with the Web Installer. The error occurs frequently after a Windows 10 Anniversary Update.</p> <p>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.</p>	26739
<p>An empty page is displayed in the Internet Explorer if the Operations Support Web Portal is opened with the URL.</p> <p>The Operations Support Web Portal is supposed to be run on an intranet site and the setting <b>Display intranet sites in Compatibility View</b> is set on the web server.</p> <p>Solution: Extend the section &lt;system.webServer&gt; in the Web Portal's configuration file (web.config). Enter an attribute or compatibility mode.</p> <pre data-bbox="201 898 491 1352"> &lt;system.webServer&gt;     ...     &lt;httpProtocol&gt;         &lt;customHeaders&gt;             ...             &lt;add name="X-UA-Compatible" value="IE=11" /&gt;             ...         &lt;/customHeaders&gt;     &lt;/httpProtocol&gt; &lt;/system.webServer&gt; </pre>	750376
<p>Target system synchronization does not show any information in the Manager web application.</p> <p>Workaround: Use Manager to run the target system synchronization.</p>	30271
<p>It is not possible to log out of the Web Portal using OAuth 2.0/OpenID Connect because it is rerouted to a false address.</p> <p>Cause: If, in the configuration parameter <b>QER   Person   OAuthAuthenticator   LogoutEndpoint</b>, a URL without a parameter is given, the logout parameters are appended to the URL in the configuration parameter in a format incompatible with the browser.</p> <p>Solution: Add a dummy parameter to the URL in the configuration parameter, for example, instead of <b>http://localhost/IdentityManager/logout</b> use the</p>	30999

Known Issue	Issue ID
value <b>http://localhost/IdentityManager/logout?from=logout</b> .	
The validity of a password, connecting the Password Reset Portal through the application server, is not tested until it is saved. The test script, invalid name components and the password history are not taken into account in the client-side test. A server-side test is done when the password is saved. Therefore, errors are not shown until the password is saved.	31354

**Table 12: Target system connection**

Known Issue	Issue ID
Memory leaks occur with Windows PowerShell connections, which use Import-PSSession internally.	23795
<p>After synchronizing an SAP R/3 environment, assignments of single role to SAP user accounts are labeled as pending.</p> <p>This problem can occur if:</p> <ul style="list-style-type: none"> <li>• SAP role assignments to user accounts were loaded in the One Identity Manager database before installing One Identity Manager 7.0.1</li> <li>• Single role assignments, which are included in collective roles, were mapped as direct assignments (Error ID 3218196)</li> </ul> <p>By resolving this problem in One Identity Manager 7.0.1, incorrect assignments are labeled as pending after synchronizing again using the appropriate synchronization configuration.</p> <p>Solution: Delete pending assignments in One Identity Manager target system synchronization.</p>	
<p>By default, the <b>HR_ENTRY_DATE</b> building block of an SAP HCM system cannot be called remotely.</p> <p>Solution: Make it possible to access the <b>HR_ENTRY_DATE</b> building block remotely in your SAP HCM system. Create a mapping for the EntryDate schema property in the Synchronization Editor.</p>	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
<p>Error in IBM Notes connector (Error getting revision of schema type ((Server))).</p> <p>Probable cause: The IBM Notes environment was rebuilt or numerous entries have been made in the Domino Directory.</p> <p>Solution: Update the Domino Directory indexes manually in the IBM Notes environment.</p>	27126



Known Issue	Issue ID
<p>The SAP connector does not provide a schema property to establish whether a user has a productive password in SAP R/3.</p> <p>If this information is meant to be in One Identity Manager, extend the schema and the synchronization configuration.</p> <ul style="list-style-type: none"> <li>• Add a custom column to the table SAPUser.</li> <li>• Extend the SAP schema in the synchronization project by a new schema type that supplies the required information.</li> <li>• Modify the synchronization configuration as required.</li> </ul>	27359
<p>No passwords can be provisioned when the bind method <b>Fast Bind</b> is in use in Active Directory. The SetPassword method is therefore not available.</p> <p>The AdhocProjection process step fails with the message:</p> <pre>[System.Runtime.InteropServices.COMException] Unknown name. (Exception from HRESULT: 0x80020006 (DISP_E_UNKNOWNNAME)).</pre>	27427
<p>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.</p> <p>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.</p>	27687
<p>If an Active Directory user account has the property MailNickName, an error occurs when the mailbox is enabled.</p> <pre>[System.Management.Automation.ActionPreferenceStopException] The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set to Stop: ExternalEmailAddress is mandatory on MailUser.</pre> <p>Cause: The property MailNickName is mapped in addition in the Active Directory mapping. This causes inconsistencies in the target system from the point the user accounts are added.</p> <p>A user account of this kind appears in the Microsoft Exchange console as a mail user but without a target email address. An attempt to open this object causes an object corrupted error in Microsoft Exchange.</p> <p>Solution: Clear up inconsistencies in the affected user accounts in Active Directory and correct your Active Directory mapping.</p>	28820
<p>Error loading single objects with Windows PowerShell if the parameter Identity is used. The error can occur during provisioning of changes made to objects in Microsoft Exchange or Exchange Online, for example, and causes follow-on errors.</p>	29152

**Known Issue****Issue ID**

---

Windows PowerShell connector's message: Command yielded <count> objects but only one was expected.

Cause: Multiple objects with the same name exist.

---

Certain data is not loaded during synchronization of SAP R/3 personnel planning data that will not come into effect until later. 29556

Cause: The function BAPI\_EMPLOYEE\_GETDATA is always executed with the current date. Therefore, changes are taken into account on a the exact day.

Solution: To synchronize personnel data in advance that will not come into effect later, use a schema extension and load the data from the table PA0001 directly.

---

Error synchronizing an OpenDJ system if a password begins with an open curly bracket. 29620

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.

Solution: The LDAP server can be configured so that a hashed password of the form {<algorithm>}hash can be passed.

- On the LDAP server: Allow already hashed passwords to be passed.
- 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.

---

If an employee's central password is used as the password for their user accounts, the password is not transferred to the password history of each individual user account. Therefore, reuse of the password cannot be prevented if the password is changed manually later. 29605

Cause: An employee's central password is an encrypted value that can only be entered in the password history when it is assigned to an employee.

Recommendation:

- Only use the employee's central password for the user accounts. Changes to the password are saved in the employee's password history.  
- OR -
- Only make changes to the passwords directly in the user accounts. This saves the password modifications in the user account's password history.

---

The Oracle E-Business Suite connector converts data with an unknown data type into strings and tries to write this value to the matching schema property in the One Identity Manager schema. 30098

## Known Issue

## Issue ID

---

If there are a large number of LDAP user accounts and LDAP groups in the database, provisioning might take a very long time. A message appears in the StdIO processor log(StdioProcessor.log) during the LDAP user account and LDAP groups update.

30172

DEBUG (SystemObjectData <static>) : Creating SystemObjectData based on entity (%DisplayName% (%cn%)) columns (UID\_LDAPAccount, UID\_LDAPContainer, UID\_LDPPDomain, XObjectKey).

TRACE (SchemaElement static) : %DisplayName% (%cn%)@LDAPAccount[.GetValue (vrtScopeParentReference) returns ...

TRACE (SchemaElement static) : %DisplayName% (%cn%)@LDAPAccount[.GetValue (UID\_LDAPContainer) returns ...

Cause: No reference scope is defined so that the default scope is used for resolving references. This causes too much data to be loaded from the database.

Solution: Define an empty reference scope. This means that scopes are not calculated when references are resolved, which noticeably improves performance with larger amounts of data.

---

Inconsistencies in SharePoint can cause errors by simply accessing a property. The error also appears if the affected schema properties mapping is disabled.

31017

Cause: The SharePoint connector loads all object properties into cache by default.

Solution:

- Correct the error in the target system.  
- OR -
- Disable the cache in the file VI.Pro-jector.SharePoint.<Version>.Host.exe.config.

---

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

32149

Solution: Clean up the data.

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

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

**To disable type conversion**

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

- In the existing <configSections>:

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

- In the new section:

```
<SAP.Middleware.Connector>
    <GeneralSettings anyDateTimeValueAllowed="true" />
</SAP.Middleware.Connector>
```

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

32945

Cause:

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

Solution:

Messages in the script can be outputted using the \*> operator to a file specified in the script.

Example:

```
Write-Warning "I am a message" *> "messages.txt"
```

Furthermore, messages that are generated using Write-Warning are also written to the One Identity Manager Service log file. If you want to force a stop on error in the script, you throw an Exception. This message then appears in the One Identity Manager Service's log file.

Although the **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom** configuration parameter is set and the **TargetSystem | SAPR3 | ValidDateHandling | DoNotUsePWODate** is not set, the assignment date is not set as the first day of the validity period in assignments of SAP roles to SAP user accounts. This behavior occurs if a **Valid until** date is given for a request but no **Valid from** date.

32628

**Table 13: Identity and Access Governance**

Known Issue	Issue ID
<p>Moving a shelf to another shop and the recalculation tasks associated with it can block the DBQueue.</p> <p>Solution:</p> <p>Parent IT Shop nodes of shelves and shops cannot be changed once they have been saved.</p> <p><b>To move a product in a shelf to another shop</b></p> <ul style="list-style-type: none"> <li>• Select the task <b>Move to another shelf</b>.</li> <li>- OR -</li> <li>• Assign the product to a shelf in the new shop then remove the product assignment to the previous shelf.</li> </ul> <p>Once you have moved all the products, you can delete the shelf.</p>	31413
<p>During approval of a request with self-service, the Granted event of the approval step is not triggered. In custom processes, you can use the OrderGranted event instead.</p>	31997

**Table 14: Third party contributions**

Known Issue	Issue ID
<p>An error can occur during synchronization of SharePoint websites under SharePoint 2010. The method SPWeb.FirstUniqueRoleDefinitionWeb() triggers an ArgumentException. For more information, see <a href="https://support.microsoft.com/en-us/kb/2863929">https://support.microsoft.com/en-us/kb/2863929</a>.</p>	24626
<p>Installing the One Identity Manager Service with the Server Installer on a Windows Server does not work if the setting <b>File and Printer sharing</b> is not set on the server. This option is not set on domain controllers on the grounds of security.</p>	24784
<p>An error, TNS-12516, TNS-12519 or ORA-12520, sporadically occurs when connecting with an Oracle Database. Reconnecting normally solves this.</p> <p>Possible cause: The number of processes started has reached the limit configured on the server.</p>	27830
<p>Valid CSS code causes an error under Mono if duplicate keys are used. For more information, see <a href="https://github.com/mono/mono/issues/7455">https://github.com/mono/mono/issues/7455</a>.</p>	29607
<p>Cannot navigate with mouse or arrow keys in a synchronization log with multiple pages.</p> <p>Cause: The StimulReport.Net component from Stimulsoft handles the report as one page.</p>	29051

**Known Issue****Issue ID**

---

Memberships in Active Directory groups of type **Universal** in a subdomain are not removed from the target system if one of the following Windows updates is installed:

- Windows Server 2016 : KB4462928
- Windows Server 2012 R2 : KB4462926, KB4462921
- Windows Server 2008 R2 : KB4462926

We do not know whether other Windows updates also cause this error.

The Active Directory connector corrects this behavior with a workaround by updating the membership list. This workaround may deteriorate the performance of Active Directory groups during provisioning and will be removed in future once One Identity Manager has resolved the problem. Microsoft

---

When connecting an external web service using the web service integration wizard, the web service supplies the data in a WSDL file. This data is converted into Visual Basic .NET code with the Microsoft WSDL tools. If, in code generated in this way, default data types are overwritten (for example, if the boolean data type is redefined), it can lead to various problems in One Identity Manager.

---

In certain Active Directory/Microsoft Exchange topologies, the Set-Mailbox Cmdlet fails with the following error:

Error on proxy command 'Set-Mailbox...'

The operation couldn't be performed because object '...' couldn't be found on '...'.

For more information, see <https://support.microsoft.com/en-us/help/4295103>.

Possible workarounds:

- Connect to the Microsoft Exchange server that the user mailbox is on. Use a custom process to do this. Use the `OverrideVariables` parameter (ProjectorComponent process component) to overwrite the server (CP\_ExchangeServerFqdn variable).
- Because this problem only occurs with a few schema properties, you should consider protecting these schema properties in the synchronization project against write operations. You can set the schema properties in a custom process using the `PowershellComponentNet4` process component through a user-defined Windows PowerShell call.

# Schema changes

The following provides an overview of schema changes from One Identity Manager version 8.0.2 up to version 8.0.5.

## Azure Active Directory Module

- Column AADUser.UserPrincipalName shortened to nvarchar(400).
- Column AADGroup.Description extended to nvarchar(1024)..

# 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 8.0.4 to version 8.0.5. Apply the patches to existing synchronization projects. For more information, see [Applying patches to synchronization projects](#) on page 53.

# 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 25.

**Table 15: Modification overview**

Module	Synchronization template	Type of modification
Azure Active Directory Module	Azure Active Directory synchronization	none
Active Directory Module	Active Directory synchronization	changed
Active Roles Module	Synchronize Active Directory Domain via Active Roles	changed
Cloud Systems Management Module	Universal Cloud Interface synchronization	none
Oracle E-Business Suite Module	Oracle E-Business Suite synchronization	changed

<b>Module</b>	<b>Synchronization template</b>	<b>Type of modification</b>
	Oracle E-Business Suite CRM data	changed
	Oracle E-Business Suite HR data	changed
	Oracle E-Business Suite OIM data	changed
Microsoft Exchange Module	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (deprecated)	none
	Microsoft Exchange 2010 synchronization (v2)	none
	Microsoft Exchange 2013_2016 synchronization (v2)	none
G Suite Module	G Suite synchronization	none
LDAP Module	AD LDS Synchronization	none
	OpenDJ Synchronization	none
IBM Notes Module	Lotus Domino synchronization	none
Exchange Online Module	Exchange Online synchronization (deprecated)	none
	Exchange Online synchronization (v2)	none
SAP R/3 User Management module Module	SAP R/3 Synchronization (Base Administration)	changed
	SAP R/3 (CUA subsystem)	none
SAP R/3 Analysis Authorizations Add-on Module	SAP R/3 BW	none
SAP R/3 Compliance Add-on 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	changed
SharePoint Module	SharePoint synchronization	none
SharePoint Online Module	SharePoint Online synchronization	none
Universal Cloud Interface Module	SCIM Connect via One Identity Connect For Cloud	changed



Module	Synchronization template	Type of modification
	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 in One Identity Manager 8.0.5 for synchronization projects. Every patch contains a script, which tests whether the patch can be applied to the synchronization project. This depends on the specific configuration of the synchronization.

For more information, see [Applying patches to synchronization projects](#) on page 53.

**Table 16: General patches**

Patch ID	Patch	Description	Issue ID
VPR#32781_SCIM	Corrects the DefaultUserPassword variable	Corrects the security settings of the DefaultUserPassword variable.  This patch is applied during the One Identity Manager automatic update.	32781

**Table 17: Patches for Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#32258	Corrects the vrtparentDn schema property	Corrects the property mapping rule for mapping the vrtparentDn schema property in all maps. This ensures that object properties that are not assigned a container are correctly provisioned.	32258

**Table 18: Patches for Active Roles**

Patch ID	Patch	Description	Issue ID
VPR#32844	Support for domain functional level Windows Server 2016	Adds the functional level to Windows Server 2016 domains.	32844
VPR#32871	Removes the negation of TSInheritInitialProgram	Corrects the mapping of the edsawtsUser-ConfigInheritInitialProgram schema	32871

Patch ID	Patch	Description	Issue ID
		property in the User mapping because the value does not have to be negated anymore.	

**Table 19: Patches for Oracle E-Business Suite**

Patch ID	Patch	Description	Issue ID
VPR#32781_EBS	Corrects the DefaultUserPassword variable	Corrects the security settings of the DefaultUserPassword variable.  This patch is applied during the One Identity Manager automatic update.	32781
VPR#30464_1	Corrects support of Oracle Database editions	Deletes the CP_EBSEdition variable from the default variable set.  This patch is applied during the One Identity Manager automatic update.	30464

**Table 20: Patches for IBM Notes**

Patch ID	Patch	Description	Issue ID
VPR#32781_NDO	Corrects the DefaultUserPassword variable	Corrects the security settings of the DefaultUserPassword variable.  This patch is applied during the One Identity Manager automatic update.	32781

**Table 21: Patches for SAP R/3**

Patch ID	Patch	Description	Issue ID
VPR#32781_SAP	Corrects the TempUserPassword variable	Corrects the security settings of the TempUserPassword variable.  This patch is applied during the One Identity Manager automatic update.	32781
VPR#32584	Change SAP title handling	Updates the connector schema so that the full SAPTitle list is loaded for each language.  This patch is applied during the One Identity Manager automatic update.	32584

**Table 22: Patches for SAP R/3 personnel planning data and structural profiles**

Patch ID	Patch	Description	Issue ID
VPR#32899	Corrects the filter on the HRPerson_0709_IDEXT schema class	Changes the objects selection of the HRPerson_0709_IDEXT schema class.  This patch is applied during the One Identity Manager automatic update.	32899

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

Patch ID	Patch	Description	Issue ID
VPR#32754	Corrects the vrtPrimary <-> primary property mapping rule	Expands a condition on the vrtPrimary <-> primary property mapping rule in the User map.	32754

## Patches in One Identity Manager Version 8.0.4

**Table 24: Patches for Oracle E-Business Suite**

Patch ID	Patch	Description	Issue ID
VPR#31735	Definition of a scope for the PersonInLocality schema type.	Extends a scope definition for the PersonInLocality schema type in the One Identity Manager connection.  This patch is applied during the One Identity Manager automatic update.	31735

**Table 25: Patches for SharePoint Online**

Patch ID	Patch	Description	Issue ID
VPR#31499	Deletes the NewUrl schema property from the Site mapping.	Deletes the NewUrl schema property from the Site mapping.  This patch is applied during the One Identity Manager automatic update.	31499

**Table 26: Patches for SAP R/3**

Patch ID	Patch	Description	Issue ID
VPR#31412	Blacklist rule filter on "userInCUArole"	Sets blacklist property mapping rules in the user synchronization step of the provisioning workflow.	31412

Patch ID	Patch	Description	Issue ID
	step	This patch is applied during the One Identity Manager automatic update.	
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#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 27: Patches for the SCIM interface (in Universal Cloud Interface Module)**

Patch ID	Patch	Description	Issue ID
VPR#31733	Update the connector schema	Updates the connector schema to enable editing of object properties that were marked with a return type of <b>request</b> . These properties must be queried explicitly.	31733

### Patches in One Identity Manager Version 8.0.3

**Table 28: Patches for Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#30192	Scope definition and usage of processing method MarkAsOut-standing	Adds a scope and the processing method MarkAsOutstanding to the synchronization step trustedDomain.	30192

**Table 29: Patches for Oracle E-Business Suite**

Patch ID	Patch	Description	Issue ID
VPR#30464	Support for Oracle Database Editions	Adds a variable to the Oracle Database Edition configuration.	30464

**Table 30: Patches for Microsoft Exchange**

Patch ID	Patch	Description	Issue ID
VPR#31026	Optimizes revision filtering	Reloads the target system schema and replaces the revision counters whenChangedUTC and whenCreatedUTC with vrtRevision.	31026

**Table 31: 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

**Table 32: Patches for Exchange Online**

Patch ID	Patch	Description	Issue ID
VPR#30498	Removes property mapping rules from the OwaMailboxPolicy mapping	Removes property mapping rules BoxAttachmentsEnabled, DropboxAttachmentsEnabled and GoogleDriveAttachmentsEnabled from the OwaMailboxPolicy mapping.	30498
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

**Table 33: Patches for SharePoint Online**

Patch ID	Patch	Description	Issue ID
VPR#30729	Corrects the <b>Mandatory</b> property of the SharePoint Online User.LoginName.	Corrects the <b>Mandatory</b> property of the schema property LoginName in the schema class User (all).  This patch is applied during the One Identity Manager automatic update.	30729

**Table 34: Patches for SAP R/3**

Patch ID	Patch	Description	Issue ID
VPR#30453	New property mapping rule for provisioning company data	New property mapping rule for mapping user account for provisioning company data.  This patch is applied during the One Identity Manager automatic update.	30453
VPR#30941	Blacklist rule filter on "userInCUARole" step	Defines property mapping rules to be excluded from the provisioning workflow's process step userInCUARole.  This patch is applied during the One Identity Manager automatic update.	30941

**Table 35: 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.  This patch is applied during the One Identity Manager automatic update.	30497

## Patches in One Identity Manager version 8.0.2

**Table 36: Patches for Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#29837	Active Directory site maps corrected.	Property mapping rule for object classes in the site mapping have been corrected.	29837

**Table 37: Patches for Oracle E-Business Suite**

Patch ID	Patch	Description	Issue ID
VPR#28834	Correction of processing methods in the synchronization step for direct permission assignments	Changes the processing methods in the synchronization step userInRESPDirect from MarkAsOutstanding to Delete.	28834
VPR#29711	Property mapping rule corrections	Adjusts the mapping direction if the schema property in the target system is read-only.	29711

Patch ID	Patch	Description	Issue ID
		This patch is applied during the One Identity Manager automatic update.	
VPR#29740	Adds missing processing methods in the synchronization step HR PersonInLocation	Adds processing methods Insert and MarkAsOutstanding in the synchronization step HR PersonInLocation. This patch is applied during the One Identity Manager automatic update.	29740
VPR#30096	Corrects different properties in synchronization projects for employee and organizational data.	Set the option <b>Data import</b> and correct specific employee mapping properties in synchronization projects that have been created with the project templates for HR, CRM or OIM data.	30096

**Table 38: Patches for Microsoft Exchange**

Patch ID	Patch	Description	Issue ID
VPR#29902	Remove duplicate mapping rules	Removes duplicate property mapping rules.	29902
VPR#29903	Enables synchronization buffer for schema property vrtParentAddressList	Enables synchronization buffer for schema property vrtParentAddressList in the mapping LocalAddressList.	29903
VPR#29917	Changes to the property mapping rule for the schema property ExchangeGuid in the Mailbox mapping.	Enables the option <b>Force mapping against direction of synchronization</b> on the property mapping rule for the schema property ExchangeGUID in the mapping Mailbox. The patch can be applied to synchronization projects for Microsoft Exchange 2013 and 2016.	29917
VPR#30018	Connection parameters extended by an additional variable	Extends the target system connection parameters by an additional variable, PreferredServer.	30018

**Table 39: Patches for Exchange Online**

Patch ID	Patch	Description	Issue ID
VPR#29921	Remove duplicate mapping rules	Removes duplicate property mapping rules.	29921

**Table 40: Patches for SAP R/3**

Patch ID	Patch	Description	Issue ID
VPR#29733	Apply revision filtering to user account communication data.	Applies revision filtering to the synchronization steps userComFax, userComPhone and userComSMTP.  This patch is applied during the One Identity Manager automatic update.	29733
VPR#29877	Add revision properties for different schema classes	Applies revision filtering in the synchronization steps profileInProfile, profileInRole, roleInRole, userInGrp, userHasParameter and userInProfile.  This patch is applied during the One Identity Manager automatic update.	29877
VPR#30160	Apply variable for SNC security settings to connection parameters	Applies the variable for SNC security settings to connection parameters.  Depends on patch VPR#27420 that was supplied with version 7.1.2.	30160

**Table 41: Patches for SAP R/3 personnel planning data and structural profiles**

Patch ID	Patch	Description	Issue ID
VPR#30115	Corrected various properties in synchronization projects for personnel planning data.	Sets the option <b>Data import</b> in the synchronization steps Employee and OrgEH and corrects specific mapping properties in synchronization projects that were created with the project template for personnel planning.	30115

**Table 42: Patches for the SCIM interface (in Universal Cloud Interface Module)**

Patch ID	Patch	Description	Issue ID
VPR#29844	Use of variables in the connection parameters	Uses the variables created in the synchronization project in the target system connection parameters.	29844
VPR#30002	Correction of property mapping rules in the User mapping.	Corrected property mapping rules in User mapping in synchronization projects for One Identity Connect For Cloud applications.	30002



## Patches in One Identity Manager Version 8.0.1

**Table 43: Patches for Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#27583	Support for domain functional levels 2016	Mapping of schema class domainDNS extended by the schema property msDF-ExpirePasswordsOnSmartCardOnly Accounts. Therefore, domain functional levels 2016 are supported.	27583
VPR#28863	Correction of patched synchronization projects	Corrects small differences between new synchronization projects and synchronization projects that have had patches applied to them.  This patch is applied during the One Identity Manager automatic update.	28863
VPR#29299	Corrects Active Directory site handling	Corrects import of Active Directory sites and child machines.	29299
VPR#29318	Set and remove maxPwdAge in domains	Corrects operation for resetting if maxPwdAge is set to <b>never</b> .	29318
VPR#29360	Avoid using employee mapping on insert	Marked employee mapping with <b>Only suitable for updates</b> .	29360
VPR#29410	Mapping of schema property ADSTGroup.AllowWriteMembers	Inserts a property mapping rule for the schema property AllowWriteMembers in the group map.  This patch is applied during the One Identity Manager automatic update.	29410
VPR#29603_ ADS	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system.  This patch is applied during the One Identity Manager automatic update.	29603

**Table 44: Patches for Active Roles**

Patch ID	Patch	Description	Issue ID
VPR#29318	Set and remove maxPwdAge in domains	Corrects operation for resetting if maxPwdAge is set to <b>never</b> .	29318

**Table 45: Patches for Oracle E-Business Suite**

Patch ID	Patch	Description	Issue ID
VPR#28876	Connection parameters extended	The connection parameters have been extended so that you can enter the user package for user account operations or a wrapper package.	28876
VPR#29528	Changes the definition of mandatory properties.	Updates the target system schema and corrects the definition of mandatory properties for adding new user accounts.  This patch is applied during the One Identity Manager automatic update.	29528
VPR#29543	Updates the target system schema.	Updates the target system schema for synchronizing security attribute assignments with different values to user accounts.  This patch is applied during the One Identity Manager automatic update.	29543
VPR#29565	Supplies variables for connection parameters	Connection parameters are supplied as variables.  This patch is applied during the One Identity Manager automatic update.	29565
VPR#29603_EBS	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system.  This patch is applied during the One Identity Manager automatic update.	29603

**Table 46: Patches for IBM Notes**

Patch ID	Patch	Description	Issue ID
VPR#28917	Changes the revision counter	Changes the revision counter. A new virtual schema property is used.  This patch is applied during the One Identity Manager automatic update.	28917

Patch ID	Patch	Description	Issue ID
VPR#29441	Property mapping rule corrections	Minor corrections of property mapping rules in Domain and Person mappings	29441
VPR#29603_ NDO	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system.  This patch is applied during the One Identity Manager automatic update.	29603

**Table 47: Patches for SAP R/3**

Patch ID	Patch	Description	Issue ID
VPR#29603_ SAP	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system.  This patch is applied during the One Identity Manager automatic update.	29603
VPR#29614	Corrected schema property vrtInactivePwd	Corrected the definition of the schema property vrtInactivePwd.  This patch is applied during the One Identity Manager automatic update.	29614

**Table 48: Patches for SAP R/3 personnel planning data and structural profiles**

Patch ID	Patch	Description	Issue ID
VPR#28927	Changed mapping for the employees' central SAP user account.	Corrects how to determine employees' SAP user account (USERID) and e-mail address (EMAILADDRESS)	28927

**Table 49: Patches for SAP R/3 authorization objects**

Patch ID	Patch	Description	Issue ID
VPR#29547	Updates the target system schema.	Updates the target system schema for synchronizing SAP transactions irrespective of how the translation is maintained.  This patch is applied during the One Identity Manager automatic update.	29547

**Table 50: Patches for SharePoint Online**

Patch ID	Patch	Description	Issue ID
VPR#29240A	Corrects errors in the reference resolution, part 1	Deletes all property mapping rules and object matching rules that Web.ID uses for resolving references or matching, respectively.  Prerequisite for patch VPR#29240B.  This patch is applied during the One Identity Manager automatic update.	29240
VPR#29240B	Corrects error resolving references, part 2	Creates new property mapping rules that use Web.Url for resolving references.  Depends on patch VPR#29240A.  This patch is applied during the One Identity Manager automatic update.	29240

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

Patch ID	Patch	Description	Issue ID
VPR#29454	Change group membership types	Inserts a new property mapping rule for the group membership's type.	29454
VPR#29603_ SCIM	Property IsSecretValue corrected for user account passwords.	Marks passwords as sensitive data in the target system.	29603

## Patches in One Identity Manager version 8.0

**Table 52: General patches**

Patch ID	Patch	Description	Issue ID
VPR#27304	Method "UnmarkAsOutstanding"	Sets the method <b>UnmarkAsOutstanding</b> in provisioning workflows.	27304
	Milestone 8.0	Milestone for the context <b>DPR</b> .	
	Milestone 8.0	Milestone for the context <b>One Identity Manager</b> .	

**Table 53: Patches for Azure Active Directory**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>Azure Active Directory</b> .	

**Table 54: Patches for Active Directory**

Patch ID	Patch	Description	Issue ID
VPR#27457	New schema property for domains	Extends the One Identity Manager schema and the mapping for ADSDomain by the schema property ObjectSID.	27457
VPR#27769_ ADS	Converts connection parameters	Converts connection parameter names and values. This patch is applied during the One Identity Manager automatic update.	27769
VPR#28560_ ADS	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>Active Directory</b> .	
VPR#27997	Changes group membership mapping	Extended the mapping group by additional virtual schema properties. This allows group memberships to be synchronized without having to find object SIDs through the global catalog.  This is a patch for a new function. This patch can be applied optionally.	27997

**Table 55: Patches for Active Roles**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>Active Roles</b> .	

**Table 56: Patches for Microsoft Exchange**

Patch ID	Patch	Description	Issue ID
VPR#27447	Use ObjectVersion to determine Microsoft Exchange version	Changing the Organization mapping to find the Microsoft Exchange version from the schema property ObjectVersion.	27447
VPR#28904	Adds RemoteMailbox to the excluded list	This patch modifies the member filter's excluded lists. Apply this patch if an Exchange hybrid environment exists but it not synchronized with One Identity Manager yet.	28904
	Milestone 8.0	Milestone for the context <b>Microsoft Exchange</b> .	

**Table 57: Patches for LDAP**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>LDAP</b> .	

**Table 58: Patches for IBM Notes**

Patch ID	Patch	Description	Issue ID
VPR#27769_ NDO	Converts connection parameters	Converts connection parameter names and values.  This patch is applied during the One Identity Manager automatic update.	27769
VPR#28560_ NDO	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>IBM Notes</b> .	

**Table 59: Patches for SAP R/3**

Patch ID	Patch	Description	Issue ID
VPR#27769_ SAP	Converts connection parameters	Converts connection parameter names and values.  This patch is applied during the One Identity Manager automatic update.	27769
VPR#27289	Create new rules on SAP licence	Extended mapping Licencetype to property mapping rule for the schema property Countries and Special version.	27289
VPR#28560_ SAP	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>SAP R/3</b> .	

**Table 60: Patches for SAP R/3 personnel planning data and structural profiles**

Patch ID	Patch	Description	Issue ID
VPR#28560_ SAP	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>SAP R/3 structural profile add-on</b> .	

**Table 61: Patches for SAP R/3 BI analysis authorizations**

Patch ID	Patch	Description	Issue ID
VPR#28560_SAP	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>SAP R/3 analysis authorizations add-on</b> .	

**Table 62: Patches for SAP R/3 authorization objects**

Patch ID	Patch	Description	Issue ID
VPR#27539	Remove SAPRCRange mapping and extensions	Removes SAPRCRange from the schemas, mapping and workflows.	27539
VPR#27769_SAP	Converts connection parameters	Converts connection parameter names and values.  This patch is applied during the One Identity Manager automatic update.	27769
VPR#28560_SAP	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>SAP R/3</b> .	

**Table 63: Patches for SharePoint**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>SharePoint</b> .	

**Table 64: Patches for the SCIM interface (in Universal Cloud Interface Module)**

Patch ID	Patch	Description	Issue ID
VPR#27769_SCIM	Converts connection parameters	Converts connection parameter names and values.  This patch is applied during the One Identity Manager automatic update.	27769
VPR#27860	Conversion of profile mapping	Changes the property mapping rules for the schema properties id, canonical name and distinguished name to the new schema properties added for them in the One Identity Manager schema.	27860

Patch ID	Patch	Description	Issue ID
		This patch can only be applied in synchronization projects which contain the Profiles map. This patch is applied during the One Identity Manager automatic update.	
VPR#28560_ SCIM	Converts German display names	German display names of property mapping rules and virtual schema properties are converted to English.	28560
	Milestone 8.0	Milestone for the context <b>SCIM</b> .	

**Table 65: Patches for the Universal Cloud Interface interface (in Cloud Systems Management Module)**

Patch ID	Patch	Description	Issue ID
VPR#27371	Pending change provisioning optimization	Provides a new variable and alters the scope.	27371
	Milestone 8.0	Milestone for the context <b>Universal Cloud Interface</b> .	

**Table 66: Patches for Unix**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>Unix</b> .	

**Table 67: Patches for the One Identity Manager connector**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>Database</b> .	

**Table 68: Patches for the CSV connector**

Patch ID	Patch	Description	Issue ID
	Milestone 8.0	Milestone for the context <b>CSV</b> .	

## Deprecated features

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



- Provider mode, including the associated process component `ObjectTransferComponent`.

The One Identity Manager connector can be used for transporting data between One Identity Manager databases. For more detailed information about synchronizing using the One Identity Manager connector, see the *One Identity Manager User Guide for the One Identity Manager Connector*.

- Archiving historical data using XML files (version 8.0.1 or later)
  - The following configuration parameters have been removed: **Common | ProcessState | ExportPolicy | ExportPath, Common | ProcessState | ExportPolicy | ExportServer, ProcessInfoImport | ImportPath, ProcessInfoImport | ImportServer, ProcessInfoImport | IgnoreDirectOperations** and **ProcessInfoImport**.
  - The option **FILE** has been removed from the configuration parameter **Common | ProcessState | ExportPolicy**.
  - The schedules **Export process information** and **Import process information** have been removed.
  - The processes `VID_Export_ProcessInfo` and `VI_ProcessInfo_Import` have been removed.
  - The process tasks `ExportProcessInfo` and `ImportProcessInfo` have been removed from the process component `ScriptComponent`.

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

- Oracle Database as database system for the One Identity Manager database (no longer available as of release One Identity Manager version 8.1)

**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/>.

## 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

One Identity Manager supports the following database systems:

- SQL Server
- Oracle Database

Processor	8 physical cores 2.5 GHz+ <b>i</b>   <b>NOTE:</b> 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM
Hard drive storage	100 GB
Operating system	Windows operating systems Following versions are supported: <ul style="list-style-type: none"><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later</li><li>• Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later</li></ul> UNIX and Linux operating systems <ul style="list-style-type: none"><li>• Note the minimum requirements of operating system vendors for Oracle databases and SQL Server databases.</li></ul>
Related Applications	SQL Server <ul style="list-style-type: none"><li>• SQL Server 2016 Standard Edition, Service Pack 2 with the current cumulative update</li><li>• SQL Server 2017 Standard Edition with the current cumulative update</li><li>• Compatibility level for databases: SQL Server 2016 (130)</li><li>• Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended)</li></ul> <b>i</b>   <b>NOTE:</b> The SQL Server Enterprise Edition is recommended on performance grounds.

---

## Oracle Database

- Oracle Database 12c Standard Edition or Enterprise Edition Version 12.1.0.2 and later

The patch level differs depending on the system platform.

**i** **NOTE:** It strongly recommended you apply the patches for Oracle bugs 18097476 (Doc ID 1683819.1) and 19497286 ( Doc ID 19497286.8)

- Character set unicode (AL32UTF8); parameter NLS\_LENGTH\_ SEMANTICS with the value **CHAR**
- 

## 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 systems Following versions are supported: <ul style="list-style-type: none"><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later</li><li>• Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later</li></ul> Linux operating systems <ul style="list-style-type: none"><li>• Linux operating system (64 bit), supported by the Mono project or Docker images provided by the Mono project.</li></ul>
Additional software	Windows operating systems <ul style="list-style-type: none"><li>• Microsoft .NET Framework Version 4.5.2 or later</li></ul> <p><b>i</b> <b>NOTE:</b> Microsoft .NET Framework version 4.6.0 is not supported.</p>

---

**i** | **NOTE:** Take the target system manufacturer's recommendations for connecting the target system into account.

Linux operating systems

- Mono 4.6 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 systems <ul style="list-style-type: none"><li>• Windows 10 (32-bit 64-bit) with at least version 1511</li><li>• Windows 8.1 (32-bit or 64-bit) with the current service pack</li><li>• Windows 8 (32-bit or 64-bit) with the current service pack</li><li>• Windows 7 (32-bit or non-Itanium 64-bit) with the current service pack</li><li>• Windows Vista with the current service pack</li></ul>
Additional software	<ul style="list-style-type: none"><li>• Microsoft .NET Framework Version 4.5.2 or later</li></ul> <p><b>i</b>   <b>NOTE:</b> Microsoft .NET Framework version 4.6.0 is not supported.</p>
Supported browsers	<ul style="list-style-type: none"><li>• Internet Explorer 11 or later</li><li>• Firefox (Release Channel)</li><li>• Chrome (Release Channel)</li><li>• Microsoft Edge (Release Channel)</li></ul>

---


## Minimum Requirements for the Web Server

Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB

---

Operating system	<p>Windows operating systems</p> <ul style="list-style-type: none"> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later</li> <li>• Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later</li> </ul> <p>Linux operating systems</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Additional software	<p>Windows operating systems</p> <ul style="list-style-type: none"> <li>• Microsoft .NET Framework Version 4.5.2 or later <ul style="list-style-type: none"> <li>•  <b>NOTE:</b> Microsoft .NET Framework version 4.6.0 is not supported.</li> </ul> </li> <li>• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.5.2 and Role Services: <ul style="list-style-type: none"> <li>• Web Server   Common HTTP Features   Static Content</li> <li>• Web Server   Common HTTP Features   Default Document</li> <li>• Web Server   Application Development   ASP.NET</li> <li>• Web Server   Application Development   .NET Extensibility</li> <li>• Web Server   Application Development   ISAPI Extensions</li> <li>• Web Server   Application Development   ISAPI Filters</li> <li>• Web Server   Security   Basic Authentication</li> <li>• Web Server   Security   Windows Authentication</li> <li>• Web Server   Performance   Static Content Compression</li> <li>• Web Server   Performance   Dynamic Content Compression</li> </ul> </li> </ul> <p>Linux operating systems</p> <ul style="list-style-type: none"> <li>• Mono 4.6 or later</li> <li>• NTP - Client</li> <li>• Apache HTTP Server 2.0 or 2.2 with the following modules: <ul style="list-style-type: none"> <li>• mod_mono</li> <li>• rewrite</li> <li>• ssl (optional)</li> </ul> </li> </ul>

# Minimum requirements for the Application Server

Processor	8 physical cores 2.5 GHz+
Memory	8 GB RAM
Hard drive storage	40 GB
Operating system	<p>Windows operating systems</p> <ul style="list-style-type: none"><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later</li><li>• Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later</li></ul> <p>Linux operating systems</p> <ul style="list-style-type: none"><li>• 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.</li></ul>
Additional software	<p>Windows operating systems</p> <ul style="list-style-type: none"><li>• Microsoft .NET Framework Version 4.5.2 or later</li></ul> <p> <b>NOTE:</b> Microsoft .NET Framework version 4.6.0 is not supported.</p> <ul style="list-style-type: none"><li>• Microsoft Internet Information Service 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.5.2 and Role Services:<ul style="list-style-type: none"><li>• Web Server   Common HTTP Features   Static Content</li><li>• Web Server   Common HTTP Features   Default Document</li><li>• Web Server   Application Development   ASP.NET</li><li>• Web Server   Application Development   .NET Extensibility</li><li>• Web Server   Application Development   ISAPI Extensions</li><li>• Web Server   Application Development   ISAPI Filters</li><li>• Web Server   Security   Basic Authentication</li><li>• Web Server   Security   Windows Authentication</li><li>• Web Server   Performance   Static Content Compression</li></ul></li></ul>

- Web Server | Performance | Dynamic Content Compression

Linux operating systems

- Mono 4.6 or later
- NTP - Client
- Apache HTTP Server 2.0 or 2.2 with the following modules:
  - mod\_mono
  - rewrite
  - ssl (optional)

## Supported data systems

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

**Table 69: Supported data systems**

Connector	Supported data systems
Connectors for delimited text files	Any delimited text files.
Connector for relational databases	Any relational databases supporting ADO.NET. <b>i</b> <b>NOTE:</b> 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 ( <a href="#">String Representation of Distinguished Names</a> ) and RFC 4512 ( <a href="#">Directory Information Models</a> ). <b>i</b> <b>NOTE:</b> Other schema and provisioning process adjustments can be made depending on the schema.
Web service connector	Any SOAP web service providing wsdl. <b>i</b> <b>NOTE:</b> 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.

## Connector Supported data systems

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	<ul style="list-style-type: none"><li>• Microsoft Exchange 2010 Service Pack 3 or later</li><li>• Microsoft Exchange 2013 Service Pack 1 or later</li><li>• Microsoft Exchange 2016</li><li>• Microsoft Exchange hybrid</li></ul>
SharePoint connector	<ul style="list-style-type: none"><li>• SharePoint 2010</li><li>• SharePoint 2013</li><li>• SharePoint 2016</li></ul>
SAP R/3 connector	<ul style="list-style-type: none"><li>• SAP Web Application Server 6.40</li><li>• SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, and 7.69</li><li>• SAP ECC 5.0 and 6.0</li><li>• SAP S/4HANA On-Premise-Edition</li></ul>
Unix connector	Supports the most common Unix and Linux derivatives. For more information, see the <a href="#">Authentication Services</a> specifications.
IBM Notes connector	<ul style="list-style-type: none"><li>• Lotus Domino Server version 8.0 up to Lotus Domino Server version 10.0</li><li>• In the client version, IBM Notes client 8.5.3 and 10.0 are supported.</li></ul>
Native database connector	<ul style="list-style-type: none"><li>• SQL Server</li><li>• Oracle Database</li><li>• SQLite</li><li>• MySQL</li><li>• DB2 (LUW)</li><li>• CData ADO.NET Provider</li><li>• SAP HANA</li></ul>
Mainframe connector	<ul style="list-style-type: none"><li>• RACF</li><li>• IBM i</li><li>• CA Top Secret</li><li>• CA ACF2</li></ul>
Windows PowerShell	<ul style="list-style-type: none"><li>• Windows PowerShell version 3 or later</li></ul>



## Connector Supported data systems

---

connector	
Active Roles connector	<ul style="list-style-type: none"><li>• Active Roles 6.9, 7.0, 7.2, 7.3.1</li></ul>
Azure Active Directory connector	<ul style="list-style-type: none"><li>• Microsoft Azure Active Directory</li></ul>
SCIM connector	Cloud applications, which recognize the System for Cross-domain Identity Management (SCIM) specification in version 2.0.
Exchange Online connector	<ul style="list-style-type: none"><li>• Microsoft Exchange Online</li></ul>
G Suite Connector	<ul style="list-style-type: none"><li>• G Suite</li></ul>
Oracle E-Business Suite connector	<ul style="list-style-type: none"><li>• Oracle E-Business Suite System versions 12.1 and 12.2</li></ul>
SharePoint Online connector	<ul style="list-style-type: none"><li>• Microsoft SharePoint Online</li></ul>

## 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

- NOTE:** To install One Identity Manager 8.0.5 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:**

- 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 8.0.5. Otherwise the schema update cannot be completed successfully.
- Note the following for automatic software updating:
  - Automatic software updating of version 7.0 to version 8.0.5 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 version 7.0 service packs will already contain the changes to these files, and therefore, must not distributed separately.
  - Automatic software updating of version 7.1 to version 8.0.5 only works smoothly if the service pack 7.1.3 is installed.
- 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 Database before updating your One Identity Manager History Service. Run the following command as administrator:

```
sc delete "HDBService"
```

**To update an existing One Identity Manager installation to version 8.0.5**

1. Run the all 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:** 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.

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) End the One Identity Manager Service on the update server.

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

5. Check whether the database's compatibility level is set the **130** and change it if necessary.

6. Run the One Identity Manager database schema update.

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

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) 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.

e. Check the One Identity Manager Service's login data. Revert to the original

settings if the One Identity Manager Service did not initially use the local system account for logging in. Enter the service account to use.

8. Start the One Identity Manager Service on the update server.

9. 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 8.0.5**

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 53.

### **To update an application server to version 8.0.5**

- 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 8.0.5**

**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 monitoring site `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 the Operations Support Web Portal to version 8.0.5**

1. Copy the contents of the folder `Modules\QER\dvd\AddOn\Operations Support Web Portal` to the installation directory for the Operations Support Web Portal, for instance `OperationSupport`.
2. Copy the following file in the folder `bin` into the Web Portal application install directory.
  - `Modules\QER\install\bin\QER.WebRuntime.WebApi.dll`
  - `Modules\QBM\install\bin\QBM.CompositionApi.Web.dll`

### **To update the Manager web application to version 8.0.5**

1. Uninstall the Manager web application
2. Reinstall the Manager web application.
3. The Manager default user requires write access to the Internet Information Services web application installation directory so that Manager web applications can be updated automatically. Check that the correct permissions are allocated.

## **Applying patches to synchronization projects**

**⚠ CAUTION:** Patches do not change customizations in synchronization projects. This means 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 update existing synchronization projects, the connection parameters from the default variable set are always used. Ensure that the variables in the default variable set contain valid values.

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

### **To apply patches**

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Edit | Update synchronization project** 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. If necessary, 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 23
- [Patches for synchronization projects](#) on page 25

## **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 2017.0011.0004.0500 for all modules and the application version 8.0 2017-11-04-417 indicate that this version is installed.

This patch updates all files that shipped with One Identity Manager 8.0.

# Additional resources

Additional information are available in:

- [One Identity Manager Support](#)
- [One Identity Manager Online documentation](#)
- [One Identity Manager Community](#)
- [One Identity Manager Training portal website](#)

## Globalization

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

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

The release is localized in the following languages: German

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

## About us

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

## Contacting us

For sales or other inquiries, such as licensing, support, and renewals, 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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product



**Copyright 2020 One Identity LLC.**

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

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

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

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

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




**Patents**

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

**Trademarks**

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

**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.**