

# One Identity Manager 9.0 Cumulative update 2

## Release Notes

**28 April 2023, 08:32**

These release notes provide information about the cumulative update 2 for One Identity Manager 9.0. Only selected resolved issues as defined by One Identity are available.

## Information about this cumulative update

This cumulative update resolves issues that were found after the release of One Identity Manager 9.0. The minimum version required for the installation of this cumulative update is 9.0.

## Resolved issues

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

**Table 1: General**

Resolved issue	Issue ID
The Starling Connection connector module can now use an application server connection to connect to the One Identity Manager database.	288784
Insufficient permissions for end users.	366596, 36021

Resolved issue	Issue ID
Error running the QBM_PJobCreate_H0Insert procedure if a <b>WhereClause</b> property changes.	368109, 36062
Some SQL statements that only query data still require a database connection with write access. Under certain circumstances, errors can occur when read access distribution is used in the cluster.	386996, 36137
If the functionality for read access distribution in a cluster is used, a message appears stating that the Database Agent Service is not running although it was started.	387007, 36120
Hierarchically structured changes labels are not displayed correctly in the Database Transporter when transporting by change label.	387008, 36115
Special change labels are not displayed when changes are committed in the Designer.	393500, 36190
Transports might be imported in the wrong order.	393501, 36194
If a column was marked for recording historical data in the source database but is removed again before it is transferred to the History Database, the History Database transfer fails.	393502, 36205
Template are not applied again if multiple objects are selected.	393506, 36223
DBQueue Processor post-processing is not always completely stopped.	393510, 36254
Multiple start times for a schedule are not taken into account correctly when calculating the run times and while running.	393512, 36263
If the server function for a process step changes, the system does not notice that the process needs to be recompiled.	393515, 36281
If a schedule is supposed to run on a certain day of the week, an error occurs when calculating the next run.	393516, 393517, 36287, 36290
After indexing tables as part of maintenance tasks, not all indexes may be released again.	393518, 36292
Machine roles are not correctly applied in the Docker container for the API Server.	393525, 36277
If parallelization of process handling is intensive, the Job queue can enter an inconsistent state when processes are restarted.	399720, 36367
Process steps in the Job queue sporadically have an inconsistent state and cannot be processed.	399723, 36382

Resolved issue	Issue ID
Filter queries for menu items that contain objects with certain starting characters are run too often.	399728, 36405
Improved performance when processing DBQueue Processor tasks.	399729, 36408
Under certain circumstances, processes that should be exported together to a History Database are not grouped into a process group.	400796, 36438
Under certain circumstances, such as when the network is interrupted, the Database Agent Service plugin stops and does not start again.	400796, 36469
Improved security for filter queries in the SCIM plugin.	403959, 36487
Empty application tokens are no longer set in Docker containers anymore.	405096, 36522
Authentication via <b>WindowsHttpAuthentication</b> does not work in the One Identity Manager Service.	407473, 36552
Trusted SQL statements are not classified as trusted if the risk index is more than or equal to 1.0.	407474, 36561
Country and timezone data has been updated.	407478, 36597
Error saving requests if processes are already in the Job queue that can trigger events to send mail for other requests.  Error message: String or binary data would be truncated in table 'OneIM.sys.TT_QBM_YParameterList_6A941822', column 'Parameter1'.	410403, 36622
Replacing variables from the navigation in element descriptions on overview forms does not work.	412470, 36683
DBQueue Processor processing is re-started too frequently.	413622, 36672
The import of schema changes with the Database Transporter may not be completed because the DBQueue Processor tasks are not processed correctly.	415846, 35858

**Table 2: Web applications**

Resolved issue	Issue ID
In the Web Portal, it is possible to save invalid conditions for automatic memberships (dynamic roles). This causes an error.	305110, 36715
Under certain circumstances, it is not possible to add products to request templates in the Web Portal.	319131, 386663, 36719,

Resolved issue	Issue ID
	36355
Under certain circumstances, the Password Reset Portal shows the splash screen all the time.	322939, 36409
It is not possible to log in to the Administration Portal using OAUTH authentication.	332087, 36360
In the Web Portal, it is not possible to publish application entitlements.	332393, 36057
In the Web Portal, the <b>Requests submitted by other users</b> filter option in the request history does not work.	332423, 36069
If you change the title of a web application it causes follow-up problems.	352481, 36016
Under certain circumstances, errors occur when displaying potential rule violations in the shopping cart.	366940, 36415
The Web Portal returns an error if a product is requested for multiple employees but the request is not permitted for at least one of them.	367180, 36070
In the Web Portal, it is possible to add products in the shopping cart although the recipient does not have request authorization.	367187, 36412
In the Web Portal, approval decisions about policy violations can only be made once.	367251, 36411
In the Web Portal, policy descriptions are not translated.	367441, 36071
Improved security of One Identity Manager HTML applications.	385798, 36178
In the Administration Portal, the links to some of the web applications are incorrect.	386166, 36530
Under certain circumstances, the Operations Support Web Portal does not display provisioning processes.	386554, 36147
Under certain circumstances, dependencies of multiple request parameters to one another are not taken into account in the Web Portal.	386868, 36143
Under certain circumstances, an error occurs when editing the date fields.	387324, 36166
The Dojo Toolkit has been updated to version 1.17.3.	387671, 36188
In the Web Portal, you cannot display the details of request templates.	388710, 36356

Resolved issue	Issue ID
Too many database connections are established in the Web Designer Web Portal for unauthorized queries.	388843, 36116
The Operations Support Web Portal does not translate all the user interface captions of the <b>Pending provisioning processes</b> function correctly.	389068, 36362
Under certain circumstances, errors occur in the Web Portal when editing the conditions of an attestation policy.	389279, 36769
In the Web Portal, it is not possible to assign to policy collections to new attestation policies.	390235, 36414
Improved performance in the Web Portal.	392694, 36229
Renewed login to a web application again does not change the <code>imx_sessiongroup</code> cookie.	393075, 36317
Under certain circumstances, the Web Designer Web Portal does not show a change icon when values are added or changed.	393467, 36230
In the Operations Support Web Portal, there are permissions missing to handle processes in a <b>Frozen</b> state.	393468, 36237
In the Web Portal, it is only possible to manage directly subordinate identities.	393484, 36325
Under certain circumstances, selecting requests in the Web Portal can lead to long response times for administrators of organizations and business roles.	393522, 36316
In the Administration Portal, it is not possible to disable the <b>Service items without image inherit the image of the assigned service category</b> configuration key.	393570, 36413
Grouping attestation cases in an attestation run's details in the Web Portal causes an error.	393864, 36359
The wrong title is displayed on the Web Portal's login page.	393883, 36323
Under certain circumstances, password questions cannot be edited in the Web Portal.	395047, 36410
In the Web Portal, copying attestation policies causes an error.	399716, 36090
If you group attestation cases of an attestation run in the Web Portal, the wrong attestation cases are shown.	399901, 36718
Under certain circumstances, the numerical values of the following config-	400775,

Resolved issue	Issue ID
uration parameters are not read in correctly.	36348
<ul style="list-style-type: none"> <li>• QER   ITShop   Recommendation   ApprovalRateThreshold</li> <li>• QER   ITShop   Recommendation   PeerGroupThreshold</li> <li>• QER   ITShop   Recommendation   RiskIndexThreshold</li> <li>• QER   ITShop   PeerGroupAnalysis   ApprovalThreshold</li> </ul>	
Under certain circumstances, the Web Portal's request history shows request properties with the incorrect values.	400793, 36357
Displaying an identity's main data causes an error in the Web Designer Web Portal.	405073, 36578
In the Web Portal, attestation cases are offered to identities for approval although their approval is not required anymore.	405092, 36505
Under certain circumstances in the Web Designer Web Portal, you cannot export the request history data.	405199, 36095
The Web Portal displays a number instead of a string for the <b>Gender</b> property in the details of an attestation run.	405318, 36529
The Web Designer Web Portal does not display all the tiles correctly.	405574, 36015
Reports show data for which the report creator does not have any permissions.	407475, 36577
In the Web Portal, if you navigate to password questions via the tiles on the home page, report subscriptions are displayed instead of password questions.	407514, 36742
When a manager selects their employees' compliance violations, the queries may take a very long time.	412471, 36684
Under certain circumstances, the Web Designer Web Portal goes into an infinite loop when an error message is displaying and closed.	413102, 36706
An error occurs in Data Explorer when listing memberships of organizations.	416107, 36835

**Table 3: Target system connection**

Resolved issue	Issue ID
There is no recalculation of the effective assignments of system entitlements for cloud target systems if the inheritance settings defined in the manage level are changed.	366536, 36020
Provisioning processes in a target system go into a <b>Frozen</b> state if a password containing special characters is transferred with encryption.	368107, 36043

Resolved issue	Issue ID
There is no recalculation of the effective assignments of system entitlements for custom target systems if the inheritance settings defined in the manage level are changed.	368108, 36045
Error changing an employee's default email address if they have an Azure Active Directory user account with an Exchange Online mailbox.	386066, 36088
When a synchronization project is created over a remote connection, an error can occur during deserialization.	386067, 36089
A synchronization simulation quits unexpectedly if a remote connection is used.	386068, 36092
PATCH operations generated for schema extension properties cause an error in the SCIM connector.	386070, 36108
A scope filter configured hierarchically in a connected LDAP target system with a Microsoft implementation (Active Directory Lightweight Directory Service (AD LDS) or Active Directory) has no effect.	386994, 36141
If the One Identity Manager database is encrypted, the system mistakenly encrypts the ExpirePassword connection parameter in synchronization projects with the LDAP connector for IBM RACF.	386997, 36136
In the Active Roles connector, an error occurs when data is read over a remote connection.	386998, 36130
Error loading objects lists via remote connections.	387001, 36128
When a synchronization project is created via a remote connection, an error can occur if the volume of data is too big.	387005, 36123
In the Synchronization Editor, the timeout for a remote connection is too short. For example, this can cause errors when a synchronization project is created via a remote connection.	387009, 36112
<p>The timeout has been increased to 3 minutes to solve the issue. If this timeout is not sufficient, you can adjust the following value in the SynchronizationEditor.exe.config file.</p> <pre>&lt;remoting&gt;   &lt;add key="RequestTimeout" value="180" /&gt; &lt;/remoting&gt;</pre>	
An error occurs updating LDAP synchronization projects.	391784, 36286
Error message: Error running the Apply' script of patch (VPR#33513 - Support multiple domains with the same DN)!	
Ineffective memberships in cloud groups or system entitlements are provisioned.	393460, 36150

Resolved issue	Issue ID
A patch with the patch ID VPR#36150 is available for synchronization projects.	
In the UNSAccount proxy table, the AccountName column for the EX0MailBox, EX0MailContact, and EX0MailUser tables is empty.	393461, 36163
Errors can occur when writing the synchronization log.	393462, 36168
A conversion error occurs for Oracle.ManagedDataAccess.Types.OracleDecimal when objects in a table are added in a sequence.	393463, 36195
An error occurs when objects in a table are added in a sequence. Error message: No suitable key property found for reloading!	393464, 36196
In the Synchronization Editor, the start up configuration list that can be assigned to a start up sequence is empty.	393466, 36226
If Active Directory is synchronized using a special variable set, an error occurs when Active Directory SIDs are updated by the MaintainOtherSid process task.	393477, 35824
Certain SAP communication data such as preferred telephone numbers or preferred email addresses that are marked as outstanding, cannot be deleted during target system synchronization.	393479, 36264
It is possible that new objects do not display meaningful values if they were incompletely mapped.	393481, 36283
The DBQueue Processor removes Active Directory user accounts from Active Directory groups that have the <b>Read-only memberships</b> property (ADSGroup.HasReadOnlyMemberships).	393485, 36327
If a value is found when loading a data set or a partition that cannot be mapped under .Net, an error occurs, and loading stops. If during synchronization, the schema type comparison quits.	393486, 36331
The Manager does not display the menu items for user accounts and groups of cloud target systems correctly.	393493, 36155
An error occurs when the Synchronization Editor performs a consistency check on schedules with multiple start times.	393496, 36164
Connecting to an Azure Active Directory tenant with schema extensions for types that are not currently supported by the Azure Active Directory connector ("device" for example) causes an error. Error message: Object reference not set to an instance of an object.	393497, 36170
Dynamic memberships of Azure Active Directory user accounts in Office 365 groups that are marked as outstanding cannot be deleted by target system	393498, 36180



Resolved issue	Issue ID
synchronization.	
If a scope file was defined, an error occurs adding new objects with the SCIM connector because of an incorrect query.	393503, 36211
Single roles contained in collective roles cause errors with double entries in the One Identity Manager database when synchronizing SAP role assignments to user accounts in a CUA.	393505, 36218
It is not possible to select an account definition for the Active Directory domain on the Microsoft Exchange mailbox or the Exchange hybrid remote mailbox forms.	393507, 393511, 36228, 36257
No OneLogin user accounts can be assigned to employees.	393508, 36241
Passwords are not transferred to the target system if the LDAP connector (V2) is being used.	393513, 36271
The <b>ADS_PersonHasTSBAccountDef_Autocreate_</b> <b>ADSAccount/Contact</b> process goes into a <b>Frozen</b> state in the <b>Wait until dependent objects recalled</b> process step.	393519, 36298
If errors occur loading target system objects, synchronization quits even though the workflow has the <b>Continue on error</b> option enabled.	393521, 36311
Using the O3S_CreateO3SSite script to add SharePoint Online site collections does not work if modern authentication with a certificate is used.	393523, 36322
The Azure Active Directory connector sends unnecessary (empty) patches after a group is updated where only members or owners have changed.	395016, 36345
The filters generated in the SCIM connector for resolving references are not formatted correctly.	395017, 36347
Active Directory user accounts and groups cannot be deleted if they are connected to a SharePoint user account.	395018, 36354
LDAP user accounts and groups cannot be deleted if they are connected to a SharePoint user account.	395018, 36354
Unnecessary updates are triggered by the LDAP connector if there are empty values.	399721, 36372
Filters in the SCIM connector may not contain sufficient data to query objects in the target system.	399722, 36379
Virtual properties for resolving references attempt to use the synchronization buffer in target systems.	399724, 36392
Error provisioning object changes if the DPRProjectionObjectState table	399725,

Resolved issue	Issue ID
contains object references with the <code>System.Byte[]</code> object type. Error message: The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or an illegal character among the padding characters.	36399
Sometime the calculation of assignment from cloud user accounts to cloud groups fails.	399726, 36404
It is not possible to enter multiple lines of encrypted data in the Synchronization Editor.	400797, 36440
The list of permitted values for group claims of Azure Active Directory app registrations was incomplete.	400798, 36441
The columns <code>AADTokenIssuancePolicy.Definition</code> , <code>AADHomeRealmDiscoveryPolicy.Definition</code> , <code>AADTokenLifetimePolicy.Definition</code> , and <code>AADActivityBasedTimeoutPolicy.Definition</code> now have the <b>Multiline</b> option.	400799, 36442
The <b>User account is disabled</b> property for user accounts ( <code>LDAPAccount.AccountDisabled</code> ) is not taken into account in the LDAP connector (V2). A patch with the patch ID VPR#36450 is available for synchronization projects.	400800, 36450
Error in the SAP Hana synchronization template in the Database Systems Integration module that allows a synchronization project to be created.	402369
An error occurs creating the <b>Send as</b> and <b>Full access</b> mailbox permissions for Microsoft Exchange remote mailboxes.	403275, 36456
Insert operation take a very long time if the SCIM provider does not support searching with filters at end points.	403276, 36459
Process steps for setting permissions and publishing are not carried out if the home directory of Active Directory user accounts with unknown home directory paths is moved.	403280, 36470
Provisioning assignments of SAP BI user account to BI analysis authorizations takes a very long time and sends a lot of RFC queries to the SAP application server.	403281, 36474
Support for non-default SQL port in Microsoft SQL databases in the Database System Integration module.	403664
Error during delta synchronization of Azure Active Directory group memberships.	403957, 36481
If an SAP schema extension was defined on a table that contains columns longer than the buffer size of 512 bytes, an error occurs when the data is	403960, 36489

Resolved issue	Issue ID
loaded via the target system browser. The error only occurs if columns are part of the results.	
Error loading objects if a schema extension for an SAP R/3 synchronization project has a key property defined that is longer than 70 characters.	403961, 36491
The delta synchronization is sporadically started with a Microsoft Teams synchronization project instead of the Azure Active Directory synchronization project.	405091, 36497
An error occurs when multiple custom target system user accounts or groups are selected in the Manager.	405095, 36512
Error loading an object list via the SCIM connector if a single object contains a syntax error.	407476, 36580
Error synchronizing a cloud application with the SCIM connector when filters are defined in the synchronization project.	407477, 36590
The value in the AADUser.ThumbnailPhoto column is not provisioned in the target system.	408362, 36586
Mailbox statistics are output twice by the Microsoft Exchange connector if data availability groups (DAG) are used.	410408, 36662
An error occurs when objects are deleted with the One Identity Manager connector and the object was already deleted by a concurrent process.	410409, 36665
If several synchronization projects exist for a target system, the provisioning tasks might be generated incorrectly for the wrong (inactive) project.	410413, 36671
When templates for mail-enabled Azure Active Directory groups are reused, it changes the AADGroup.IsSecurityEnabled and AADGroup.IsMailEnabled columns.	413104, 36713
Error during provisioning, if a script property was added to the SCIM target system's extended schema that tries to write to the target system.	413620, 35372
If a Microsoft Teams team is archived, the associated SharePoint Online page can still be edited.	413623, 36677
When memberships are removed from Unix groups, other memberships that should not be removed are deleted.	413624, 36679
SAP user account assignments to SAP roles are not updated correctly if the structure of the SAP roles changes.	413625, 36701
The handling of outstanding Exchange Online email users generates unnecessary provisioning tasks for Azure Active Directory groups.	413626, 36707

**Table 4: Identity and Access Governance**

<b>Resolved issue</b>	<b>Issue ID</b>
Permissions missing from the <b>vi_4_ITSHOPADMIN_OWNER</b> permissions group for the columns <code>ADSGroup.HasReadOnlyMemberships</code> and <code>AADGroup.HasReadOnlyMemberships</code> .	386065, 36078
Application entitlements that are created automatically might not have a display name.	386069, 36094
Sporadically, there are double entries in the auxiliary table for request procedures ( <code>PW0HelperPWO</code> ).	386995, 36139
If request parameters are given for a request, the UUIDs are displayed in the request history instead of the parameters' display names.	392643, 36207
If the display pattern for the Person table is customized such that the <code>InternalName</code> column is not used anymore, errors occur when generating email notifications for the next approver.	393465, 36214
DBQueue Processor requests <code>CPL-K-ComplianceSubRuleFillPersonS</code> block each other, are reset repeatedly, and are not processed.	393482, 36297
If an approval decision is made when a request is created, no email notification is sent to the requester.	393483, 36318
Error adding a parameter to a newly added request property if the Manager is running via an application server.	393492, 36153
If an approval workflow is run through when a dependent product that requires prior external approval is requested, the corresponding event for the dependent product is not generated.	393494, 36157
The <code>CreateITShopOrder</code> method for creating assignment requests for memberships in Exchange Online mail-enabled distribution groups is missing.	393495, 36160
The <code>TSBVPersonAndGroups</code> view can contain duplicates. For example, this can cause errors generating reports about the origin of entitlements.	393499, 36187
Office 365 groups are not taken included when determining the origin of entitlements.	393504, 36217
The Analyzer cannot run an analysis after the database connection has changed.	393509, 36253
If the <b>QER   ITShop   ExceededValidUntilUnsubscribe</b> configuration parameter is set, unsubscribing processes quit unexpectedly with an error.	393514, 36274
Under certain circumstances, those responsible for organizations are not deleted. <ul style="list-style-type: none"> <li>An application role is assigned to a department as an additional manager.</li> </ul>	393520, 36301

Resolved issue	Issue ID
<ul style="list-style-type: none"> <li>An employee becomes a member of this application role by assignment request.</li> <li>The assignment is canceled.</li> </ul> <p>However, the employee remains manager of the department (entries in the HelperHeadOrg table with XOrigin = 8 are not deleted).</p>	
End users are missing edit permissions for the AttestationHistory table.	393526, 36302
Error attesting objects with properties that are disabled by a pre-processor conditions.	394881, 36370
An error occurs if multiple attestation runs are created simultaneously for an attestation policy. Only one attestation run is created. The processes to generate further attestation runs fail.	399719, 36364
The <b>ReducedApproverCalculation</b> configuration parameter is not taken into account when determining the fallback approver.	403958, 36483
Approval procedures stop responding when the number of approvers is set to <b>-1</b> .	405090, 36443
Error displaying extended properties in the Manager if the CIM module for Cloud Access Governance is installed.	406761
Error calculating memberships in dynamic groups. Error message: The current transaction cannot be committed and cannot support operations that write to the log file.	407472, 36531
In some cases, an error occurs when transporting approval workflows. Error message: PWODecisionStep: Write permission denied for value "CountApprover".	410404, 36641
In some module, the origin of entitlements determined correctly when assigning user account directly to groups.	410405, 36646
If a product is moved to another shelf, renewal requests are not reset.	413621, 36634
Poor performance loading the list of attestation cases.	413631, 36739
Events on the Person base object are not generated properly if management of an employee's role memberships (like the primary department) is automated via IT Shop requests.	413634, 36614

**Table 5: Data Governance Edition**

Resolved issue	Issue ID
An error occurs in the Web Designer Web Portal when an attempt is made to select alternative Active Directory groups for approving a resource access request.	304997
The Data Governance Service Configuration Wizard log is not generated.	413216

## List of resolved issues in previous cumulative updates of One Identity Manager

### Solved issues in cumulative update 1

**Table 6: General**

Resolved issue	Issue ID
Performance problems using the QER_FTPW0OrderPerson SQL table function on the SQL Server 2019 and compatibility level (150) for SQL Server 2019 databases.	35882
Under certain circumstances, the end user is missing permissions for the following generated functions, although the permissions are given correctly in the QBMDBRightsAddOn table. <ul style="list-style-type: none"> <li>• QER_FTEntitlementSourceWho</li> <li>• QER_FTEntitlementSourceWhy</li> <li>• QER_FTEntitlementSourceWhat</li> <li>• QBM_FGIPrepropConditionDeactiv</li> </ul>	35921
Using the emergency stop to halt the DBQueue Processor can result in a time delay if a lot of DBQueue Processor processes are being handled quickly.	35338
Permissions required on new tables are not granted for end users if the Database Transporter imports the schema extensions.	35934
The QBM_PTtriggerDrop procedure logs entries in the system journal even though no triggers were deleted.	35949
Updating statistics during maintenance tasks caused an error. Therefore, the statistics are not up-to-date. Error message: User does not have permission to perform this action.	35960
An error occurs when the Software Loader imports a new file. Error message: Number of primary key columns does not match.	36006
An error occurs using OAuth2.0/OpenID Connect to log in to the application server and the Job server, for example to display the status.	36018
Under certain circumstances, the Database Transporter compiles web	319014

Resolved issue	Issue ID
projects too often when it imports a cumulative update.	
The Database Transporter does not display each transport of a cumulative transport correctly.	35901, 36262
Cumulative transport packages are not displayed correctly in the transport history.	36260
The DBTransporterCMD.exe program does not set back single user mode after importing a cumulative transport package.	36261

**Table 7: Web applications**

Resolved issue	Issue ID
Not all the values of an attested object are displayed by Web Portal attestation.	35855
When assigning a sample to an attestation policy, a condition was automatically created based on attestation wizard parameters. However, this was not mapped to the definition (XML), which meant that the parameters were not displayed correctly in the Web Portal.	320926
In the Data Explorer, an error occurs when listing organizations that are assigned more than one dynamic role.	321431, 35971
When creating conditions for automatic assignment of application entitlements in the Web Portal, an error occurs assigning a value to the <b>Container</b> property.	316539
If a rule violation occurs in the Web Portal when checking a shopping cart, the loading screen does not always close.	317162
In the Web Portal, if new requests are made through peer groups or reference users, the products selected through organizational structures are not added to the cart.	319781
Shelves cannot be edited in the Web Portal.	321363
The Web Portal displays the <b>Entitlement Loss</b> tab twice in an attestation case's details pane.	318807
If you make a new request in the Web Portal using a peer group, the products selected by organizational structure are each put in their own shopping cart.	320891
In the Web Portal, under certain circumstances, only the ID of the selected object is displayed when conditions for automatic membership are created instead of the display name.	321874
In the Web Portal, under certain circumstances, an error message is displayed during approval of an attestation case.	317836

Resolved issue	Issue ID
The Web Portal displays some untranslatable text when the terms of use are being accepted.	318203
In the Password Reset Portal, it is not possible to create new user accounts.	324290
In the Web Portal, no system role memberships are displayed.	324128
In the Web Portal, the wrong description text is displayed when editing request templates.	319746
In the Web Portal, it is not possible to search by compliance rules and to filter the respective search results.	323899
The Web Portal marks all pending requests as compliance violations the moment just one of the displayed pending requests causes a compliance violation.	326083
In the Web Designer Web Portal, the wrong error message is displayed if there is a connection issue.	319184
A report is not subscribable in the Web Portal if it is not configured for PDF format.	326723
When verifying assignment objects for report subscription parameters, no results are returned.	322252
The Web Portal uses the wrong identifiers in the details of an attestation case.	324279
The Web Portal does not display memberships that were added or deleted in system roles in an identity's history.	319462
Under certain circumstances, after clicking <b>Assign/Change</b> in the Web Portal, no objects can be selected for property fields.	324289
The Web Portal shopping cart does not correctly display whether an identity is not entitled to request a product. The request can still be sent, but it has no effect.	324383
Under certain circumstances, the Web Portal's search function does not work and generates an error.	327287
The Web Portal does not always show the correct results when grouping and filtering in tables at the same time.	322124
The Web Portal displays the wrong message when selecting requestable products if a product was already assigned.	319133
The Web Portal displays product dependencies incorrectly when products are added to the shopping cart.	319915
Under certain circumstances, the Web Portal shows the splash screen all the time.	322907



Resolved issue	Issue ID
In the Web Portal, when you reset objects to their previous state you can switch to the second step in the wizard without entering data. This causes an error.	322985
In the Web Portal, no recipient must be selected if requesting for others.	324118
In the Operations Support Web Portal a column title is not translated corrected in the process overview.	321613
The Web Portal does not translate all text correctly.	321535
The Web Portal does not automatically query mandatory request parameter when a service item is added to the shopping cart.	317218
The Operations Support Web Portal leaves the queue list empty, and no data appears.	323845
The Web Portal cannot display a compliance violation in the shopping cart and the respective shopping cart cannot be submitted.	326440
Error verifying or submitting a shopping cart in the Web Designer Web Portal and in the Web Portal.	35925
The Web Designer Web Portal does not check renewal requests and cancellations correctly in the shopping cart.	36131
If you enter a date for a product property in the Web Portal's shopping cart, under certain circumstances the value is deleted when the shopping cart is submitted.	35995
If you try to log in to the Web Portal with the wrong credentials, an empty page is displayed instead of an error message.	384912

**Table 8: Target system connection**

Resolved issue	Issue ID
Synchronization with OneLogin fails if there are self-registered users. Error: Null object cannot be converted to a value type.	35889
Synchronization with OneLogin sometimes reports ambiguous keys in the reference resolution to the OLGUserHasOLGCustomAttribute table.	35962
Various functions required to manage a OneLogin domain are now provided in the Manager. It is now possible to: <ul style="list-style-type: none"> <li>• Create account definitions for domains</li> <li>• Define exclusion of roles</li> <li>• Specify administrators for roles</li> <li>• Use the various reports on offer</li> </ul>	35909

Resolved issue	Issue ID
<p>Error saving a synchronization project if the connection goes through the application server and the target system connection has high network latency.</p> <p>Error message: Application server returned an error.</p>	35871
<p>If an object filter was defined for a root entry in the scope definition, there might not be an object in the scope.</p>	35880
<p>The schema provided by the Domino connector might be incomplete or individual properties might not have the correct data type.</p>	35999, 36142
<p>Access to the <b>RemoteConnectPlugin</b> does not work across machines.</p> <p>The HTTP server registration has been adjusted and can be set up using the <b>HttpAuthentication</b> and <b>HttpBindAddress</b> parameters in the plugin's configuration.</p>	35950
<p>You cannot select an account definition on the OneLogin user account's master data form.</p>	35983
<p>The <b>OLG_4_NAMESPACEADMIN_ONELOGIN</b> permissions group has too many edit permissions on OneLogin applications (OLGApplication table) and OneLogin roles (OLGRole table).</p>	35994
<p>There is no recalculation of the effective assignments of target system-specific system entitlements if the inheritance settings defined in the manage level are overwritten. The following assignments are affected:</p> <ul style="list-style-type: none"> <li>• Subscription assignments to Azure Active Directory user accounts (AADUserHasSubSku table)</li> <li>• Entitlement assignments to Oracle E-Business Suite user accounts (EBSUserInResp table)</li> <li>• Role assignments to SAP R/3 user accounts (SAPUserInSAPRole table)</li> <li>• Structural profile assignments to SAP R/3 user account (SAPUserInSAPHRP table)</li> </ul>	36014
<p>Processing conflicts between synchronization and other system processes (for example, provisioning) are not always reliably detected.</p> <p>In the StdioProcessor configuration file, the rate of updating the processing information can now be configured. By default, the data remains in the cache for <b>60</b> seconds. Only change this value if there is an issue.</p> <p>If you are affected by the issue, add the following entries to the StdioProcessor.exe.config file:</p> <pre>&lt;configSections&gt; ... &lt;section name="synchronization" type="System.Configuration.NameValueSectionHandler" /&gt;</pre>	35992

Resolved issue	Issue ID
<pre>... &lt;/configSections&gt; &lt;synchronization&gt;     &lt;add key="SysConcurrencyCacheLifeTime" value="60" /&gt; &lt;/synchronization&gt;</pre>	

**Table 9: Identity and Access Governance**

Resolved issue	Issue ID
<p>Using the predefined <b>Employee attestations</b> policy collection causes long running calculations and over-complicated attestation cases.</p> <p>A sample was defined for the policy collection that allows the number of employees to attest to be limited. Therefore, only the employees assigned to the sample along with their memberships, user accounts, and system entitlements are attested.</p> <p><b>IMPORTANT:</b> For the following default attestation procedures, the snapshot of the referenced objects was limited to those objects that are specified in the object relations 1-3:</p> <ul style="list-style-type: none"> <li>• Attesting primary departments</li> <li>• Certification of users</li> <li>• Attesting user accounts</li> </ul> <p>This reduces the processing time and the memory requirements.</p> <p>If other information about attestation is required, the contents of the snapshot can be adjusted accordingly.</p>	35845
When creating a new attestation policy, an initial condition is no longer set.	35867
Under certain circumstances, entries in the PWOHelperPW0 table are not recalculated.	35972
Duplicate entries in the AttestationHelper table. Sporadically, entries are created twice in the auxiliary table for attestation cases (AttestationHelper). This means the number of email notifications is doubled. If the approval workflow contains an approval step for external approval, the process for external approval is generated twice.	36000

**Table 10: Data Governance Edition**

Resolved issue	Issue ID
After upgrading from One Identity Manager Data Governance Edition 9.0 you might see the following error message if, in the Manager, users try to access the <b>Managed hosts</b> .	319605

Error: QAM.Common.Exceptions.ExternalException: VI.Base.ViException: Potentially dangerous behavior was detected. The request will be ignored.

## Applicability of this cumulative update

Table 11: Products affected by this cumulative update

Product name	Version	Platform
One Identity Manager	9.0	All those supported

## Upgrade and installation instructions

**NOTE:** Ensure that automatic software update is enabled. Otherwise the cumulative update cannot be applied in full. For more information about the automatic software update, see [Automatic updating of One Identity Manager](#).

**NOTE:** If you migrate the One Identity Manager database again with version 9.0 to add or remove a module, for example, then you must also apply the cumulative update afterward.

The following files are deployed for the cumulative update.

- **Install.CU.exe:** Use the **Cumulative Update Installer** wizard to install the cumulative update. The wizard guides you through each step. First the wizard updates the components of your locally installed One Identity Manager. Then the Database Transporter updates your One Identity Manager database.
- **Install.CU.cmd.exe:** You can use this program to update the components of your locally installed One Identity Manager from the command line. Run the update using the command line console as administrator.
- **OneIdentityManager.9.0.CU02.Transport.zip:** This file contains the transport package with resolved issues.
- **OneIdentityManager.9.0.CU.ReleaseNotes.pdf:** Contains detailed information about resolved issues.
- **OneIdentityManager.9.0.CU.ReleaseNotes\_de-de.pdf:** Contains detailed information about the resolved issues in German.

To install the cumulative update, the following actions are performed.

1. Update of the locally installed One Identity Manager components on the administrative workstation.

2. Update of the One Identity Manager database.
3. (Optional) Update of the synchronization project.

A cumulative update can deploy patches for synchronization projects. You must apply these patches to the 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.

See also:

- [Installing this cumulative update](#) on page 21
- [Applying patches to synchronization projects](#) on page 23

## Installing this cumulative update

**NOTE:** Test changes in a test system before installing the cumulative update in a production system. Use a copy of the production database for testing.

### *To install the cumulative update with the Cumulative Update Installer*


1. Put the following files in a temporary directory on your administrative workstation.
  - Install.CU.exe
  - OneIdentityManager.9.0.CU02.Transport.zip
2. Start the Install.CU.exe file from the temporary directory.

This starts the cumulative update.
3. On the start page, select the installation language and click **Next**.
4. On the **Update Settings** page, select the directory with the One Identity Manager installation you want to update and click **Next**.

This starts installing the transport package.
5. If there are still active processes, that are using files from the target directory, these processes are displayed in the **Running processes** page.
  - Use the **End process** context menu item to end the processes to allow the installation to start.
6. On the **Installation** page you can see the installation's progress.

After the components have been successfully installed, the Database Transporter starts.

**NOTE:** The next steps queue the calculation tasks for the DBQueue Processor. Ensure that the Database Agent Service is running. If you have stopped the One Identity Manager Service, which also runs the Database Agent Service, you must start the server again. Otherwise internal calculation tasks cannot be carried out and the transport package import quits with errors.

7. On the **Update the database with CU transport** page, select the database connection and authentication for logging in to the database. Select a user who at least has administrative permissions for the One Identity Manager database.
    - To connect to the database, click **Next**.
  8. The **Install cumulative updates** page shows the import steps to be run and the progress of the import. The import procedure can take some time.
    - After successful installation, click **Next**.
  9. To end the program, click **Finish** on the last page.
- | NOTE:** Use the  button to save any errors that occur whilst importing.

### ***To install the cumulative update from the command line***

1. Put the following files in a temporary directory on your administrative workstation.
  - Install.CU.cmd.exe
  - OneIdentityManager.9.0.CU02.Transport.zip
2. Run the component update using the command line console as administrator. Use -h to show the program help.

Example call:

Install.CU.cmd.exe

```
-S="OneIdentityManager.9.0.CU02.Transport.zip"
-D="C:\Programs\One Identity\One Identity Manager"
```

with:

- -S: Name of the transport package.
  - -D: Local directory of the One Identity Manager installation to be updated with the cumulative update.
3. To update the One Identity Manager database from the command line, use the DBTransporterCMD.exe program. Run the database update from the command line console. Use -? to show the program help.

Select a user who at least has administrative permissions for the One Identity Manager database.

Example call:

DBTransporterCMD.exe

```
/File="C:\Temp\OneIdentityManager.9.0.CU02.Transport.zip"
/Conn="Data Source=<Database server>;Initial Catalog=<Database name>;User ID=<Database user>;Password=<Password>"
/Auth="Module=DialogUser;User=<User name>;Password=<Password>"
```

with:

- /File: Path to the transport file.
- /Conn: Database connection parameter. Select a user who at least has administrative permissions for the One Identity Manager database.
- /Auth: Authentication data. The authentication data depends on the authentication module used.

## Applying patches to synchronization projects

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

### *Before you apply a patch*

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

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

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

### *To apply patches*

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Edit > Update synchronization project** menu item.
3. Click **Apply selected patches**.
4. Enter any user input as prompted.
5. Use the patch log to check whether customization need to be reworked.
6. If required, rework customizations in the synchronization configuration.
7. Run a consistency check.
8. Simulate the synchronization.
9. (Optional) Activate the synchronization project.
10. Save the changes.

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

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

## Verifying successful installation

### *To verify that the cumulative update is installed*

- Start the Designer or the Manager and select the **Help > Info** menu item.  
The **System information** tab gives you an overview of your system configuration.  
The version number 9.0.02.0 for all modules indicates that this cumulative update is installed.

## Removing this cumulative update

Once installed you cannot remove this cumulative update.

## Long Term Support (LTS) and Feature Releases

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

### Long Term Support (LTS)

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

### Feature Release

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

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



**Table 12: Comparison of Long Term Support (LTS) Release and Feature Release**

Category	Long Term Support (LTS) Release	Feature Release
Release frequency	Every 36 months (includes resolved issues and security related updates).	Approximately every 12 months (includes resolved issues and security related updates).
Duration of full support	36 months	18 months
Duration of limited support	12 months (after the end of full support)	6 months (after the end of full support)
Versioning	All versions where the second number is <b>0</b> . For example: 9.0.0 (9.0.1, 9.0.2,), 10.0.0, 11.0.0, and so on.	All versions where the second number is not <b>0</b> . For example: 9.1.0 (9.1.1, 9.1.2), 9.2, 9.3, and so on.
Duration of service pack availability between releases	Approximately every 6 months, cumulative updates (CUs) are expected for each LTS release.	Every 6 months patch releases (service pack) are expected for each feature release currently supported.
Criteria for issuing hotfixes for LTS outside of a cumulative update cycle	<ul style="list-style-type: none"><li>• The product is not functioning after installing the most recent CU and the customer cannot wait until the next CU is available.</li><li>• The product is not functioning/is inoperable which is causing a production outage/serious issue.</li><li>• A security related fix is needed on a priority basis to address a vulnerability.</li><li>• No fixes will be issued to implement an enhancement outside of the cumulative update cycle.</li></ul>	

Release details can be found at [Product Life Cycle](#).

One Identity strongly recommends always installing the latest revision of the selected release path (Long Term Support path or Feature Release path).

## Moving between LTS versions and Feature Release versions

You can move from an LTS version (for example, 9.0 LTS) by installing a later feature release or version (for example 9.2). Once this has happened, you are not on the LTS

support path until the next LTS base version (10.0, etc.) is installed.

You can move from a Feature Release to an LTS Release, but only to an LTS release with a later version. For example, you cannot move from 9.2 to 9.0 LTS. You have to keep upgrading with each new Feature Release until the next LTS Release version is published. For this example, you would wait until 10.0 LTS is available.

## Patches

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

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

For customers on the feature release option track, maintenance releases are cumulative, meaning that maintenance releases do not need intermediate releases to be installed to update to a newer maintenance release. This is unchanged from previous versions. For example, if you want currently use version 9.1.1 and want to upgrade to 9.2, and, for example, versions 9.1.3, 9.1.4, and 9.1.5 have been released, you only have to install version 9.2 and it automatically applies the resolved issues from 9.1.3, 9.1.4, and 9.1.5.

## Frequently Asked Questions (FAQs)

What is Long Term Support (LTS)?

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

What are the benefits to being on an LTS release?

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

What are the disadvantages to being on an LTS release?

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

Duration of an LTS release

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

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

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

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

- Yes. You can do this by installing a later maintenance version or feature release. For example, if you currently have version 9.0 (LTS) and decide to move to 9.2, you will come off the LTS support path until you install the next base LTS version (10.0, etc.)

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

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

## Additional resources

Additional information is available in:

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

## About us

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

## Contacting us

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

## Technical support resources

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

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

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

**Copyright 2023 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 highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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