# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR One Identity Manager v8.1.5.

## Maintenance Update of One Identity Manager v8.1.5.

**Maintenance Report Number: CCEVS-VR-VID11003-2022**

**Date of Activity**: January 27, 2022

**References:** Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;

Impact Analysis Report for One Identity Manager v8.1.5, v1.2, January 27. 2022

**Documentation Updated**:

The following table show how the original documentation has been updated:

| Evidence Identification | Effect on Evidence/ Description of Changes |
|---|---|
| **Security Target:**<br>One Identity Manager v8.1 Security Target Version 1.2, 3 February 2020 | **Maintained Security Target:**<br>One Identity Manager v8.1.5 Security Target Version 1.0, December 16, 2021<br>Changes in the maintained ST are:<br>• Updated identification of ST<br>• Section 1.1 - Updated TOE software version<br>• Section 2 - Updated the One Identity Manager version number<br>• Section 2.1 - Updated the One Identity Manager version number<br>• Section 2.2 - Updated the One Identity Manager version number<br>• Section 2.2.1 - Updated the One Identity Manager version number<br>• Section 2.2.2 - Updated the evaluation excluded features for the new release 8.1.5 product improvements or features. |

| Evidence Identification | Effect on Evidence/ Description of Changes |
|---|---|
| | • Section 2.3 – Identified the most current documentation for the current One Identity Manager release 8.1.5 |
| **Common Criteria Compliance Guide:**<br>One Identity Manager 8.1 Common Criteria Supplemental Admin Guidance 2020 | **Maintained Common Criteria Compliance Guide:**<br>One Identity Manager 8.1.5 Common Criteria Supplemental Admin Guidance 2021, Updated 14 December 2021<br>Changes in the maintained Guidance are:<br>• Updated identification of Guidance<br>• Added a change date: Updated - 14 December 2021<br>• Updated identification of TOE version<br>• Updated the ***To change your personal password using the Password Reset Portal*** instructions to exclude configuration of login using target system credentials (not evaluated and considered out of scope). |

## Assurance Continuity Maintenance Report:

The Leidos CCTL submitted the latest Impact Analysis Report (IAR) and Assurance Continuity Maintenance package on behalf of One Identity LLC to the CCEVS for approval on January 27, 2022. The IAR is intended to satisfy the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes

## A Summary of Changes to TOE:

The following summarizes the new features and product improvements added to One Identity Manager since the previous One Identity Manager v8.1 evaluation to v8.1.5. The changes and rationale for Minor verdicts are categorized and summarized as shown it the following table. There is some overlap between the categories.

| Category | Justification for Minor Verdicts |
|---|---|
| Basic functionality | These changes are generally for functionality that is outside the TOE in the environment. Examples are switching to Azure SQL database and 2 Factor Authentication. The ESM TOE uses the Active Directory server in the environment for authentication. There were no changes to the ST or guidance documentation, does not affect claimed security |

| | |
|---|---|
| | functionality, and has no effect on the result of any Assurance Activity test. |
| Web Applications | Examples include Hot Spot recognition, updates to connection wizards and formatting table columns. Changes to the Web Portal are not security related. These changes results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test. |
| Target system connections | Adding support for separate products does not affect the claimed SFRs in the One Identity Manager Security Target or the claimed security functionality. |
| Identity and Access Governance | The ESM TOE uses Active Directory authentication server in the environment. Examples of these changes: overview forms for application roles, and improved support for peer group analysis for attestation. These enhancements are not security relevant and does not affect the SFRs or the claimed security functionality. These features result in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test. |
| General Enhancements | Examples include performance improvements, protection from damaging SQL statements, and new field definitions. These enhancements do not affect the claimed security functionality. These features do not change the ST or guidance documentation and has no effect on the result of any Assurance Activity test. |
| General known issues Enhancement | Examples include updated support to the FileComponent and ScriptComponent processes. This enhancement is not security relevant and does not affect the SFRs or the claimed security functionality. These updates result in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test. |
| General web applications Enhancement | Examples are improvements to correct database non-conformities with ONE, job queue processes, process parameters, and options to change shopping cart priorities. These changes are not security relevant and does not affect the SFRs or the claimed security functionality. These features result in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test. |
| Identity and Access Governance Enhancement | Examples are updated to business roles and resource assignments and password creation logs in the authentication server in the environment. These enhancements result in no changes to the ST or |

| | |
|---|---|
| | guidance documentation and has no effect on the result of any Assurance Activity test. |
| Deprecated features | The following features have been deleted from the product. Oracle Database is no longer supported, Google ReCAPTCHA Version 1 is no longer supported, SvnComponent has been removed.<br>The MailNotification, DefaultCultureFormat configuration parameters are removed. Ten scripts have been removed because their functions are obsolete or no longer ensured:<br>• VI_Del_ADSAccountInADSGroup<br>• VI_GetDNSHostNameOfHardware<br>• VI_GetDomainsOfForest<br>• VI_GetServerFromADSContainer<br>• VI_Make_Ressource<br>• VID_CreateDialogLogin<br>• VI_Discard_Mapping<br>• VI_Export_Mapping<br>• VI_GenerateCheckList<br>• VI_GenerateCheckListAll |

The tables in Appendix A are summarized from the IAR. The tables provide brief explanation of the product changes. Each table categorizes changes for a particular product version from ONE v8.1.1, v8.1.2, v8.1.3, 8.1.4 and 8.1.5. Some of the changes from earlier versions are carried forward to later version tables. The redundant entries have been greyed-out to make it easier to see what changed in each version . The validation Team has reviewed the rationale for being minor and agree with the verdicts.

## Search for Known Vulnerabilities:

The CCTL claims that no CVEs were discovered and fixed during the period from the last full evaluation to 12/13/2021.

More recent public searches for new vulnerabilities was completed was performed. No vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the minor updates.

The search terms are listed below. All searches below were performed on 12/13/2021 and again on 1/24/2022.

Databases used for the searches:

- http://web.nvd.nist.gov/view/vuln/search
- https://support.oneidentity.com/identity-manager/all/alerts-notifications
- Google

Search terms

- One Identity Manager (TOE name)
- One Identity (alternate branding)
- OneIdentity (alternate branding)

- Quest One Identity Manager (previous name of product)
- Dell One Identity Manager (previous name of product)
- "One Identity Manager" vulnerability (Google search term)
- "One Identity Manager" exploit (Google search term)

## Cryptography:

No updates or changes have been made to the Cryptographic Library provided in the operational environment.

## Regression testing:

Regression testing was performed on all maintenance versions (i.e., 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5). Automated and manual testing was performed. The tests were run to verify all old and new features. Any test case failures were tracked, and all the bugs found were fixed and verified.

## Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

## Appendix A — List of Product Changes

The implementation of the features, enhancements, and depreciated features for ONE 8.1.1 shown in Table 1 resulted in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity tests. They are all judged to be Minor changes.

Table 1 Features, Enhancements, and Depreciated Features for ONE 8.1.1

| Category | Description |
|---|---|
| **Basic functionality** | Support for managed instances in Azure SQL Database. |
| | Windows Server 2019 is supported for service, web and application servers. |
| | Use the **Common \| MailNotification \| DefaultFont** and the **Common \| MailNotification \| DefaultFontSize** configuration parameters to specify font and font size for mail templates in the Mail Template Editor. |
| | In mail templates, any parameters can be used when calling a script. |
| | The **RequestWatchDogPlugin** has a new **Action** parameter (Action) to specify which action should be run when queries come to a still stand. Permitted values are **Restart** (default) and **Log**. |
| | |
| **Web Applications** | One Identity now offers users the option to log in, simply and securely, to One Identity Manager web applications with help of (physical) security keys. These security keys support the W3C standard **Webauthn**. Using them guarantees a high degree of login security. |
| | It is now possible, with the help of three Web Designer configuration keys, to specify the format of date and time input for the entire web project. |
| | The terms of use are now automatically shown in the same language as the Web Portal. |
| | |

| Category | Description |
|---|---|
| **Target system connection** | You can now synchronize departments and the employees assigned to them using synchronization projects for employee data from an Oracle E-Business Suite Human Resources module. |
| | Support for One Identity Safeguard version 2.6 and Version 2.7. |
| | Improved support of One Identity Safeguard clusters when establishing a connection. |
| | For each access request policy, a new application role is created for the owner under the **Privileged Account Governance \| Asset and account owners** application role. |
| | Microsoft Exchange 2019 with cumulative update 1 and Microsoft Exchange 2016 cumulative update 12 are supported. |
| | Microsoft Exchange linked room mailboxes are supported. |
| | The central user administration and child systems can be removed so that they subsequently become independent clients, which can be managed by One Identity Manager and administrated separately from each other. |
| | A recertified version of the One Identity Manager Business Application Programming Interface (BAPI) is available. The BAPI has reduced functionality, which works to the advantage of performance. The BAPI is no longer compatible with One Identity Manager version 6.1.x or older versions. |
| | SharePoint 2019 is supported. |
| | Execution of provisioning and single object synchronization processes as well as target specific processes can be distributed over different servers. |
| | **TECH PREVIEW ONLY**: A new LDAP connector **LDAP Connector (Version 2 -Tech Preview)** is available. |
| | |
| **Identity and Access Governance** | Support for a peer group analysis for requests.There is a new event, PeergroupAnalysis, for the PersonWantsOrg table, which can be linked into the approval workflow with an EX step. |
| **Enhancements** | **Description and Issue ID** |
| **General known issues Enhancement** | Improved performance checking columns in the QBMUniqueGroup table that must be unique by definition. |
| | Improved performance in DBQueue Processor. |
| | Improved performance processing transactions that repeatedly queue tasks in the DBQueue. |
| | In the configuration parameter Common \| MailNotification \| Signature LinkDisplay, you can specify an alternative display text for the link to your company's website for use in email signatures. |
| | Improvements in Job Queue Info. The port is taken into account when a Job server log is displayed. |
| | Support for the System Debugging on 64-bit systems. 31203 |
| | Improved login checks. Using the Common \| Authentication \| SessionsPerUserAndMinute configuration parameter, you can specify the number of sessions a user can open within a short space of time. The default value is 10. If this number is exceeded, the user is sent a message. |
| | Third-party components update. |
| | Improved security for the One Identity Manager Service API. 31542 |
| | Improved protection of the application server's API. |
| | Improved protection against damaging SQL statements. |
| | Improved performance in the vQBM_PGUIDReplaceLight procedure. |

| Category | Description |
|---|---|
| | |
| **General web applications Enhancement** | In the Web Portal, all the application roles a person is responsible for are managed under Responsibilities \| My Responsibilities \| One Identity Manager application roles. |
| | In the Web Portal, under **My profile \| Contact data \| Language for value formatting**, users can specify how dates and numbers are formatted. |
| | Improved error message if there is no approval policy available for delegating. |
| | To prevent user sessions being stolen, the session ID is no longer given in the HTML code. The web application must run in Release mode for this. |
| | Improved security for dealing with column filters. |
| | |
| **Target system connection** | Improved performance reloading objects from the database. |
| | If the option **Ignore undefined values** is set for a schema property, a message appears in the synchronization log if the connector tries to write a non-defined value. |
| | Operation for memberships are recorded with more detail in the synchronization log. |
| | If the connector schema in a synchronization project was extended by using a schema extension file, the schema extension can be viewed and edited in the target system wizard after it has been saved. |
| | Access restrictions for the Azure Active Directory User.CompanyName schema property has been removed. CompanyName can now be written to. |
| | Improved grouping of Azure Active Directory user accounts in the Manager. |
| | Improved performance provisioning Active Directory groups, containers and domains. |
| | Improved performance by correcting object filters in Active Directory project templates. |
| | The behavior of Active Directory processes has been changed with respect to load balancing of processes for provisioning and single object synchronization as well as target system specific processes on different Job servers. |
| | Improved performance loading synchronization objects from Microsoft Exchange if revision filtering is used. |
| | Improved performance loading synchronization objects from Exchange Online if revision filtering is used. |
| | Improved performance provisioning Notes policies and certificates. |
| | Improved performance provisioning SAP user accounts. |
| | Improved performance deleting memberships in SAP roles. |
| | Improved split algorithm in the SAP connector if WHERE clauses in external schema extensions are very long. |
| | The LDAP connector support schema with Base64 coded content. |
| | The LDAP connector supports reading of auxiliary class attributes that were assigned in the object class schema through the auxiliaryClass attribute. |
| | The LDAP connector is more tolerant toward entries that are not RFC compliant. |
| | The RACF connector supports the auxiliary class RacfUserCsdataSegment. |
| | The process function RunAgent of the process component NDO Component has been extended by an additional parameter of type **OUT**. |
| | The **TargetSystem \| SAPR3 \| Accounts \| CalculateLicence** configuration parameter can be used to specify whether to calculate SAP system measurement for SAP user accounts. |
| | Improved performance synchronizing SAP cost centers. |

| Category | Description |
|---|---|
| | Improved performance by correcting object filters in SAP project templates. |
| | The SCIM connector supports passing of the specified scope for the token requested by OAuth 2.0. |
| | Improved performance by correcting scope filters in Oracle E-Business Suite project templates. |
| | |
| **Identity and Access Governance Enhancement** | Improved process monitoring of requests. The configuration parameter **Common \| ProcessState \| UseGenProcIDFromPWO** controls whether the GenProcID of an IT Shop request is retained for the entire approval process. |
| | The documentation for inheriting company resource through system roles and the effect of exclusion definitions has been comprehensively reworked ().*One Identity Manager System Roles Administration Guide* |
| | Improved performance processing requests of approvers that are automatically approved. |
| | Improved performance deleting customers with requests, from the IT Shop. |
| | Improved performance moving requests. |
| | The reminder interval and the timeout for attestation approval steps are checked every 30 minutes by default. The interval can be specified in the **Checks reminder interval and timeout of attestation cases** schedule. |
| | |
| **Deprecated features** | Oracle Database is no longer supported as a database system for the One Identity Manager database. |
| | Google ReCAPTCHA Version 1 is no longer supported. |
| | The process component SvnComponent has been removed. |
| | The **Common \| MailNotification \| DefaultCultureFormat** configuration parameter has been deleted. |
| | The following scripts have been removed because their functions are obsolete or no longer ensured:<br>• VI_Del_ADSAccountInADSGroup<br>• VI_GetDNSHostNameOfHardware<br>• VI_GetDomainsOfForest<br>• VI_GetServerFromADSContainer<br>• VI_Make_Ressource<br>• VID_CreateDialogLogin<br>• VI_Discard_Mapping<br>• VI_Export_Mapping<br>• VI_GenerateCheckList<br>• VI_GenerateCheckListAll |
| | |

The implementation of the features, enhancements, and depreciated features for ONE 8.1.2 shown in Table 2 resulted in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity tests. These features are not security relevant. They are all judged to be Minor changes.

Table 2 — Features and Enhancements Introduced or Deprecated in One Identity Manager 8.1.2

| Category | Description |
|---|---|
| **Basic functionality** | Support for SQL Server 2019 with the compatibility level for databases **SQL Server 2016 (130)**. |

| Category | Description |
|---|---|
| | As from One Identity Manager version 8.1.2, a new method is available for updating customer databases faster. This method is only implemented for updating the schema in the context of service packs. For initial schema installation and updating the schema to a new main version, the conventional method is still used. |
| | Support for custom staging levels for the One Identity Manager database. |
| | |
| **Web applications** | In the Web Portal, you can display and request products that other people from your vicinity have already requested. |
| | In the Web Portal, you can specify how dates and numbers are formatted. You can configure this in the **My Profile \| Contact Data \| Language for value formatting** field. |
| | You can configure the Password Reset Portal such that you can log in using user accounts other than the central user account with help of password questions or a passcode. |
| | |
| **Target system connection** | One Identity Safeguard Version 2.8, Version 2.9, Version 2.10, and Version 2.11 are supported. |
| | Microsoft Exchange 2013 with cumulative update 23 is supported. |
| | **TECH PREVIEW ONLY**: A new LDAP connector **LDAP Connector (Version 2 -Tech Preview)** is available. Tech Preview connectors are not included in the evaluated configuration |
| | |
| **Identity and Access Governance** | Use the **QER \| Person \| UseCentralPassword \| CheckAllPolicies** configuration parameter to specify if an employee’s central password is checked against all the target system’s password policies of the employee’s user accounts |
| | Approvers that are registered for Starling Two-Factor Authentication, can also use the Starling 2FA app for approvals. Multi-factor (2-factor) authentication was excluded in the previous evaluation. |
| | Support for peer group analysis for attestation. |
| **Enhancements** | |
| **General** | Improved performance transferring deleted Job queue entries to the process history. |
| | Improved performance of DBQueue Processor tasks for shrinking records from process monitoring and the process history. |
| | Improved performance processing DBQueue Processor tasks with large amounts of data. |
| | Improved performance processing DBQueue Processor tasks during synchronization. |
| | Improved performance deleting objects including all their dependencies. |
| | Improved performance executing deferred operation with large amounts of data. |
| | Improved performance updating current UTC offsets of all timezones. |
| | Columns that need to be in a defined display pattern in the table are given implicit viewing permissions. |
| | Improved compilation of HTML applications in the Configuration Wizard. |
| | Improved documentation for applying scripts about conditional displaying and editing of columns. |
| | Improved how to determine the current version of the database server to display in the system configuration report. |
| | Improved accessing the One Identity Manager History Database when connected through an application server. |
| | New consistency checks test whether or not there is a deferred operation that has already been triggered but does not have a process in the Job queue. |

| Category | Description |
|---|---|
| | Improved the **Objectkey references to non existing object** and **Objectkey references to non existing object (tolerated)** consistency checks. |
| | You can specify a priority for registering a customizer method |
| | The **Fallback connection** option (QBMConnectionInfo.IsFallBackAppServer) for the process generation connection data can only be enabled for one application server. |
| | Improved identification of expiring sessions on the application server. |
| | Improved reestablishing connections to the application server. |
| | Improved protection against damaging SQL statements. |
| | Improved error messages when transporting changes if an error occurs while implementing them in the target database. |
| | New MergeAction parameter in the DBTransporterCMD.exe command line program for handling merge conflicts during a transport. |
| | The ScriptComponent process component has two new process functions available to it, ScriptExecExclusive and ScriptExecExclusive32, for executing scripts exclusively for one object. |
| | Improved accessibility in the Manager. |
| | Improved how permitted and not permitted character classes for password policies are displayed on forms in the Manager and the Designer. |
| | Improved how translations are displayed in the **Edit translation** dialog. |
| **General web applications** | |
| | Improved security for dealing with column filters in the Web Portal. |
| | Improved performance making approval decisions for request and attestations in the Web Portal. |
| | Improved performance of certain database queries in the Web Portal. |
| | Removed checkbox in front of the date field in the Web Portal. If you do not want a time restriction, do not enter anything in the field. |
| | When an API is compiled, it is tested to see if a ConfigureAwait(false) method has been used for each await keyword. This ensures that asynchronous code is applied correctly. |
| | Webauthn security keys: The RSTS version has been updated to version 2019.11.22.0. You can prevent the **X-Frame-Options** HTTP response header from being returned by setting the **DisableAddingXFrameOptionsHeader** configuration setting to **true**. |
| | Improved performance of grid controls. Less database queries are generated. |
| | The Web Portal monitor page has been reworked and now shows better information. |
| | Improved performance of database-bound grids. |
| | In the Web Portal, the system role's Hyper View has been reworked. |
| | On the Web Portal's start page, assignment resources, multi-requestable/unsubscribable resources, and resources are now visible in the **My Responsibilities** tile. |
| | Improved performance displaying requestable products in the Web Portal. |
| | Improved performance requesting products in the Web Portal. |
| | |
| **Target system connection** | Only relevant project templates are offered in the project wizard. |
| | Synchronization of objects with incorrect object properties can be allowed if necessary. |
| | Improved performance synchronizing Microsoft Exchange recipient lists. |

| Category | Description |
|---|---|
| | The Oracle E-Business Suite connector recognizes on its own, which Oracle Database Editions are used in the target system. |
| | Improved performance provisioning assignments of Oracle E-Business Suite entitlements to user accounts. |
| | During provisioning of G Suite user accounts, user accounts are prevented from being processed in parallel. |
| | During provisioning of Notes objects, the latency is increased after the index is refreshed to be able to reload object properties without errors. |
| | In the One Identity Safeguard connector, the version of the Windows Power-Shell module in use is checked to see if it is supported and matches the appliance. If this is not the case, the connection is closed with an appropriate error message. |
| | Support for Telnet session request for PAM. |
| | The SAP connector now uses SAP code pages 6100, 6200, and 6500. |
| | Accelerated synchronization of personnel planning data from an SAP HCM system. |
| | New USOBHASH schema type in the SAP connector schema to load permissions from the USOBHASH table in SAP R/3. |
| | The SCIM connector now allows parallel access 10 times max. to load single objects during synchronization. |
| | Improved performance using the SCIM connector for synchronization. |
| | The CSV connector now takes language settings into account when reading and writing. |
| **Identity and Access Governance** | |
| | When a passcode is created, it is logged in the system journal. |
| | Business roles that are used in assignments resources cannot be deleted anymore. |
| | Improved performance calculating QER_FTPWOVisibleForPerson. |
| | The **Retain service item assignment on relocation** option can now be set on default service items. |
| | |
| **Deprecated features** | Same as for 8.1.1 |

The implementation of the features, enhancements, and depreciated features for ONE 8.1.3 shown in Table 3 resulted in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity tests. These features are not security relevant. They are all judged to be Minor changes.

Table 3 — Features and Enhancements Introduced or Deprecated in One Identity Manager 8.1.3

| Category | Description |
|---|---|
| Basic functionality | Improved support for encrypting a database |
| | To support troubleshooting in OAuth 2.0/OpenID Connect authentication you can log personal login data, such as information about tokens or issuers configuration parameter defines whether the login data is recorded. |
| | Running of all automatic schedules can be temporarily stopped. |
| | |
| Web Applications | In the Web Portal, you can now use heatmaps to show how many requests have been generated for each department, cost center, location or business role. |
| | In the Web Portal, it is now possible to control how table columns are sorted by using the keyboard. |

| Category | Description |
|---|---|
| | |
| Target system connection | One Identity Safeguard version 6.0 is supported. |
| | Simplified system connection wizards for Active Roles. |
| | Support for dynamic Azure Active Directory groups. |
| | Support for dynamic Office 365 groups. |
| | HCL Domino Server Version 11 and HCL Notes Client Version 11.0.1 are supported. |
| **Enhancements** | **Description and Issue ID** |
| General | The FileComponent process component support path lengths of more than 260 characters. 30846 |
| | New parameters of the ScriptComponent process component are available for the CSVExport and CSVExportSingle process tasks. |
| | More tolerant handling of temporary errors in the schema update. |
| | Improved functionality for the Launchpad. |
| | You can now enter more than one value in the **TargetSystem \| LDAP \| Authentication \| RootDN** configuration parameter using a pipe (\|) delimited list. |
| | Improved error logging in the application server. |
| | |
| General web applications | In the Web Portal, keyboard shortcuts for buttons are now displayed in full (for example, **[Alt-C]**). |
| | In Web Portal, the version number is shortened (for example 8.1). |
| | In the Web Portal, the option to change the priority of all products when you edit the shopping cart has been renamed. |
| | Improved performance when checking the shopping cart in the Web Portal. |
| | Improved security generating reports in the Web Portal. |
| | Improved support for HTTP header authentication if the connection goes through an application server. |
| | Improved accessibility in the Web Portal when displaying tiles in high contrast mode. |
| | The Microsoft.OData library has been updated to the newest version. |
| | If API resources (Typescript client and Swagger JSON) are not required for compiling the API, the API resources can now be generated in the DbCompiler.exe file using the DoNotBuildResources parameter. |
| | The information saved in the sessions cookies of an API Server session now expire if the customer restarts the browser. |
| | |
| Target system connection | Improved error messaging for load operations in the synchronization log. |
| | 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. |
| | Improved performance provisioning G Suite user accounts. |
| | You can configure which user data is transferred to a different user account before G Suite user accounts are deleted. |
| | Improved documentation of permissions required for integrating One Identity Manager as an application in Azure Active Directory. |
| | The filter for the HRPerson_0709_IDEXT schema class was changed from a string to an integer comparison. |
| | Improved messages for the SCIM connector in the synchronization log. |
| | The SCIM connector detects whether the service provider requires URLs with a closing slash. |

| Category | Description |
|---|---|
| | The recommendations from Microsoft about avoiding throttling during SharePoint Online synchronization have been implemented. |
| | The Active Directory connector can use the One Identity Manager Service's user account to log in on the target system. To do this, leave the login credentials on the project wizard's **Login** page empty. |
| | The Microsoft Exchange connector can use the One Identity Manager Service's user account to log in on the target system. To do this, in the project wizard enable the **Use account of One Identity Manager Service** option on the **Enter connection credentials** page. |
| | In the project wizard for connecting cloud applications in the Universal Cloud Interface, the cloud application menu has been made larger. |
| | In an SAP schema extension file, you can provide a time offset for the revision counter (AddRevisionTimeOffset attribute) in the schema type definition. |
| | Adjustments required to the Exchange Online connector due to Microsoft turning off functionality in the cloud. |
| | You can configure whether the database to be connected takes case sensitivity into account for the generic ADO.NET provider. |
| | Improved performance calculating user account assignments to groups in custom target systems (UNSAccountBInUNSGroupB table). |
| | |
| Identity and Access Governance | Improved performance creating and by approval of attestation cases. |
| | Improved indexing of the PersonHasObject and BaseTreeHasObject tables. |
| | 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. |
| | Improved support for peer group analysis for attestation. |
| | |
| **Deprecated features** | Oracle Database is no longer supported as a database system for the One Identity Manager database. |
| | Google ReCAPTCHA Version 1 is no longer supported. |
| | The process component SvnComponent has been removed. |
| | The **Common \| MailNotification \| DefaultCultureFormat** configuration parameter has been deleted. |
| | The following scripts have been removed because their functions are obsolete or no longer ensured:<br>• VI_Del_ADSAccountInADSGroup<br>• VI_GetDNSHostNameOfHardware<br>• VI_GetDomainsOfForest<br>• VI_GetServerFromADSContainer<br>• VI_Make_Ressource<br>• VID_CreateDialogLogin<br>• VI_Discard_Mapping<br>• VI_Export_Mapping<br>• VI_GenerateCheckList<br>• VI_GenerateCheckListAll |

The implementation of the features, enhancements, and depreciated features for ONE 8.1.4 shown in Table 4 resulted in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity tests. These features are not security relevant. They are all judged to be Minor changes.

Table 4 — Features and Enhancements Introduced or Deprecated in One Identity Manager 8.1.4

| Category | Description |
|---|---|
| Basic functionality | New configuration option for detection and mail notification if the One Identity Manager Service stops processing queries. |
| | |
| Target system connection | Support for One Identity Active Roles version 7.3.3, version 7.4.1, and version 7.4.3. |
| | |
| Identity and Access Governance | Support for OAuth 2.0 authentication for Exchange Online mailboxes using attestation by mail and approval by mail. |
| **Enhancements** | **Description and Issue ID** |
| General | Extended the scope of SQL logging if SQL queries need to be repeated. |
| | Exceptions that caused the SQL query retries are logged. |
| | Improved testing of multiple name properties in password policies if the **Name properties denied** option is set. |
| | Improved performance for various SQL functions. |
| | Improved performance transferring to the History Database. |
| | Reduced processing time in the DBQueue due to optimized setting of automatically generated calculation tasks. |
| | Optimized internal database communication to coordinate processing of DBQueue Processor tasks. |
| | |
| General web applications | Improved performance determining the service items used for requests in the Web Portal. |
| | In the Web Portal, empty date fields are now shown with an example value so that you can quickly identify the expected date format. |
| | The following Java Script libraries have been updated:<br>● Bootstrap: Version 3.4.1<br>● AngularJS: Version 1.7.9 |
| | |
| Target system connection | In the Manager, the general data form for target system types shows the AdditionalSystemTypes (**Alternative connectors**) column. |
| | The SCIM connector supports SCIM provider cookies in REST queries. |
| | The SAP connector supports setting of current passwords for login using Secure Network Communications (SNC) with Single Sign-On. |
| | Corrected SAP companies reference to SAP user account for SAP S/4HANA 2.0 support. |
| | Improved display of test results if the SCIM endpoint connection is tested in the system connection wizard for cloud applications. |
| | Improved logging of native database connectors when establishing a database connection using the generic ADO.NET provider. |
| | |
| **Deprecated features** | Oracle Database is no longer supported as a database system for the One Identity Manager database. |
| | Google ReCAPTCHA Version 1 is no longer supported. |
| | The process component SvnComponent has been removed. |
| | The **Common \| MailNotification \| DefaultCultureFormat** configuration parameter has been deleted. |

| Category | Description |
|---|---|
| | The following scripts have been removed because their functions are obsolete or no longer ensured:<br>● VI_Del_ADSAccountInADSGroup<br>● VI_GetDNSHostNameOfHardware<br>● VI_GetDomainsOfForest<br>● VI_GetServerFromADSContainer<br>● VI_Make_Ressource<br>● VID_CreateDialogLogin<br>● VI_Discard_Mapping<br>● VI_Export_Mapping<br>● VI_GenerateCheckList<br>● VI_GenerateCheckListAll |

The implementation of the features, enhancements, and depreciated features for ONE 8.1.5 shown in Table 5 resulted in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity tests. These features are not security relevant.  They are all judged to be Minor changes.

Table 5 — Features and Enhancements Introduced or Deprecated in One Identity Manager 8.1.5

| Category | Description |
|---|---|
| Basic Functionality | The system information overview shows whether a database is encrypted. |
| | In the Database Compiler and in the program's status bar, a warning is shown if there are invalid script assemblies. The database needs to be compiled. |
| | To access the REST API on the application server, the user required the **Enables access to the REST API on the application server** (AppServer_API). |
| | The search index on the application server supports indexing of diacritical characters. |
| | To prevent maintenance tasks from obstructing daytime relevant post-processing in the DBQueue, a new QBM_PDBQueueProcess_Mnt on <database> database schedule has been implemented for processing the maintenance tasks. |
| | The effectiveness of the assignments (XIsInEffect column) is recorded in the history. |
| | |
| Target system connection | Support for One Identity Active Roles version 7.4.4. |
| | The Exchange Online connector uses the Exchange Online PowerShell V2 module. |
| **Enhancements** | **Description and Issue ID** |
| General | Improved protection against damaging SQL statements. 33586, 33587 |
| | The Launchpad **Configure > Add system users** entry has been renamed to **Configure > Manage system users**. |
| | Columns of assignment tables (M:N tables, M:all tables) cannot be included in the full-text search (DialogColumn.IndexWeight). |
| | In the Schema Extension, validity of the foreign key definition is checked when a read-only database view is added. |
| | Optimized performance importing schema extensions with the Database Transporter. |
| | In the Object Browser, when you switch to another object of the same type, the focus remains on the selected property. This makes it easier to compare object properties when you switch between them. |
| | Improved performance of various SQL functions. |

| Category | Description |
|---|---|
| | New mandatory field definitions for the DialogState.Ident_DialogState, DialogState.NationalStateName, DialogCountry.CountryName, DialogCountry.NationalCountryName columns. The groups of columns that must be unique (QBMUniqueGroup) have been adjusted. |
| | New optional parameter -dc (--deleteconfig) in the InstallManager.CLI.exe command line tool to remove configuration data and log files when uninstalling One Identity Manager. |
| | |
| General web applications | Logging in to the Web Portal with an OAuth provider is now possible without calling up oauth/{appId}/{authentifier} URL beforehand. |
| | Identity credentials (id_token_hint) are now passed during OAuth provider login. |
| | Improved Web Portal performance. |
| | It is now possible for a web application to communicate with an API Server other than the one that the web application comes from. |
| | The withPermissions parameter of the Web Designer dbcount() function is now marked as depreciated. |
| | Improved speed of displaying the shopping cart. |
| | Increased the Web Portal’s security. |
| | Updated the Microsoft.Owin library to version 4.1.1. |
| | |
| Target system connection | This functionality, of access permissions automatically being created for clients when SAP roles or profiles are assigned to user accounts, was removed when ID 28147 was implemented in version 8.1.0. |
| | The SAPUser.Guiflag column's display name has been changed to **Login by SAP GUI allowed (insecure communication)**. |
| | SCIM filter expressions are passed down with each subset query during cursor-based paging. |
| | The SCIM connector now supports Bearer authentication for logging in to the target system.<br>A patch with the patch ID VPR#33729 has been applied to the product for synchronization projects. |
| | Attribute check with schema during modification calls has been removed from the RACF connector. |
| | The native database connector now supports columns with the DateTimeOffset data type. |
| | The synchronization engine now differentiates between NULL and empty values when comparing. |
| | The Starling Cloud configuration wizard now supports the EU region in the One Identity Starling Cloud login. Users are automatically connected to the Starling Cloud system that suits them the best. |
| | |
| Identity and Access Governance | Improved performance calculating dynamic roles. |
| | Improved performance checking compliance rules. |
| | Improved performance in the queries that determine the approvers of default application procedures. |
| | |
| **Deprecated features** | Oracle Database is no longer supported as a database system for the One Identity Manager database. |
| | Google ReCAPTCHA Version 1 is no longer supported. |
| | The process component SvnComponent has been removed. |
| | The **Common \| MailNotification \| DefaultCultureFormat** configuration parameter has been deleted. |
| | The **TargetSystem \| NDO \| TempNetworkPath** configuration parameter has been deleted. |
| | The following scripts have been removed because their functions are obsolete or no longer ensured:<br>• VI_Del_ADSAccountInADSGroup<br>• VI_GetDNSHostNameOfHardware<br>• VI_GetDomainsOfForest |

| Category | Description |
|---|---|
| | • VI_GetServerFromADSContainer<br>• VI_Make_Ressource<br>• VID_CreateDialogLogin<br>• VI_Discard_Mapping<br>• VI_Export_Mapping<br>• VI_GenerateCheckList<br>• VI_GenerateCheckListAll |