One Identity Starling CertAccess

Release Notes

October 7, 2021

These release notes provide information about the One Identity Starling CertAccess version from October 7, 2021 release. One Identity Starling CertAccess documentation is available in both English and German. For the most recent version of the product information, see the Starling CertAccess documentation.

About this release

One Identity Starling CertAccess delivered access requests and access certifications in the form of a Software as a Service solution allow Starling CertAccess to augment One Identity Active Roles with approvals, notifications, escalations, and other business processes for your hybrid environment. Use Starling CertAccess to easily satisfy attestation and recertification policy requirements while providing auditors what they need.

Starling CertAccess is integrated as a service in One Identity Starling (https://cloud.oneidentity.com).

Starling CertAccess is a minor release with new functionality and improved behavior. See Features on page 2 and Enhancements on page 3.

Features

New features in the Starling CertAccess version from October 7, 2021:

Starling CertAccess Web Portal

- Starling CertAccess provides an Operations Support Web Portal to help you run your Starling CertAccess instance. Here you can, among other things:
  - Monitor process handling
  - Identify failed processes, deduce measures to take, rerun the processes
  - Display synchronization status and synchronization logs

  The way this works is described in the *One Identity Starling CertAccess Operations Support Web Portal User Guide*.
- Starling CertAccess administrators are notified daily about failed processes. You can disable email notifications in the Web Portal.

See also:

- Enhancements on page 3
- Resolved issues on page 6

List of new features in previous versions of Starling CertAccess

New features in the version from June 17, 2021

- Starling Governance has been renamed to Starling CertAccess.
- In Starling CertAccess Agent, you can now edit the list of system entitlements that are not automatically assigned to the IT Shop after synchronizing. Therefore, the Active Directory groups listed here cannot be requested in the Starling CertAccess Web Portal.
- The Starling CertAccess IT Shop and attestation features can now be individually deactivated in the Web Portal if they are not going to be used.
- It is now possible to display attestation runs in the Web Portal. You can also display the attestation cases that belong to an attestation run and download a report that provides an overview of the state of attestation cases.

New features in the version from May 5, 2021

- Integration of business processes for handling access requests and access certifications for One Identity Active Roles as a service in One Identity Starling. These include:

    - Approval of access requests for Active Roles
    - Attestation and recertification of existing access permissions in Active Roles
    - Automatic revoking of access permissions if certifications are denied
    - Notifications about pending, granted, or denied approvals and certifications
    - Assignment of access permissions to specific identities
    - Configuration of request shop to manage access requests
- Synchronization between an Active Directory environment managed by One Identity Active Roles and Starling CertAccess through the Starling CertAccess Agent. Synchronization transfers all the required data for controlling access, such as user accounts, groups, and group memberships.
- Reports about synchronized data, available access permissions, or closed attestations.

Enhancements

The following is a list of enhancements implemented in the Starling CertAccess version from October 7, 2021.

Table 1: General enhancements

Enhancement	Issue ID
Improved logging of validating access tokens on the application server.	34485, 282235

Table 2: Starling CertAccess Web Portal

Enhancement	Issue ID
Improved display of identities' names.	34560
Improved display of reports with a history.	34566
When submitting requests, the valid until date is no longer checked against the current time. For example, errors are avoided if a long time has elapsed between creating and sending a shopping cart.	34621
• Memberships in dynamic Active Directory groups cannot be requested anymore. • After denying attestation of memberships in dynamic groups, the group membership is not automatically removed. An appropriate reason is entered in the attestation history.	34628

List of enhancements in previous versions of Starling CertAccess

Enhancements in the version from September 9, 2021

Table 3: General enhancements

Enhancement	Issue ID
Before a proof of Concept trial expires, email notifications are sent announcing the upcoming end of the 14-day test period. Notifications will be sent 3 days and 1 day before the trial period ends. Once the trial period is over, users are notified that the trial instance has been deleted and can no longer be used.	280085

Enhancements in the version from August 26, 2021

Table 4: Starling CertAccess Agent

Enhancement	Issue ID
If the SMTP server is not yet configured for sending email, in Starling CertAccess Launchpad, a corresponding icon is displayed for the **Administrative tasks > System configuration > Configure email connection** task.	34440
A time delay is now in effect when exiting the Starling CertAccess Service to allow the service to synchronize with Starling CertAccess.	34459

Table 5: Starling CertAccess Web Portal

Enhancement	Issue ID
Improved performance when assigning managers to identities in the Data Explorer.	34461

Enhancements in the version from June 17, 2021

Table 6: Starling CertAccess Agent

Enhancement	Issue ID
Improved error messages in the Starling CertAccess Service's log file.	34238, 275045
To minimize the number of email notifications sent to attestors, notifications about pending attestation cases are only sent once a day by default. This means that the **Notification by email** feature cannot be used for attestations. Email notifications about pending requests continue to be sent separately. You can configure the required behavior in the Starling CertAccess	34242, 34312

Enhancement	Issue ID
Launchpad.	
Improved documentation about the Starling CertAccess Service permissions required for synchronizing with One Identity Active Roles in the *One Identity Starling CertAccess Administration Guide for One Identity Active Roles Integration*.	34261

Table 7: Starling CertAccess Web Portal

Enhancement	Issue ID
New report: • **Auditing of requests**: This report contains a list of requests including their request history. The report is limited to a maximum of 5000 requests. • **Detailed status of an attestation run**: This report contains the status of an attestation run including an estimated time for completing the attestation.	19310, 34219
An identity cannot assigned to its manager as a manager.	19675
If attestation of user accounts that are not connected to an identity is approved, then the user accounts are not presented for attestation anymore. In the Data Explorer, user accounts that are not connected with an identity can be filtered by different categories.	33384
Improved performance creating attestation cases.	34017, 34039, 34243
The Data Explorer now shows whether a system entitlement is managed dynamically in Active Roles. Memberships in these system entitlements cannot be edited in the Web Portal.	34168, 34323, 273350
All Starling CertAccess administrators are now target system managers for Active Directory as well.	34283
You can now add images to service categories that show the requesters.	252720
Creating and editing attestation polices have been reworked and extended: • Obsolete attestation policy options are no shown anymore. • The next regular start of an attestation policy is now displayed. • Enabled attestation policies with disabled schedules are not displayed as disabled anymore.	264383, 268558, 269953
The Web Portal now supports HTTP compression.	265172
Identities can now be activated and deactivated using a button in the Data Explorer.	267002

Enhancement	Issue ID
In the Data Explorer, you can now create service items for system entitlements.	268557
In the Data Explorer, you can now display each attestation case of the system entitlements and identities.	271416
On the request shops overview page a alert is displayed if none of the system entitlements can are requestable.	272544
In the Data Explorer, the following system entitlement filters have changed: • Previous: **Published** New: **Requestable** • Previous: **Not published** New: **Not requestable**	272550
You can now download a report that provides an overview of the state of the associated attestation cases.	272657
In the Data Explorer, memberships in a system entitlement are now displayed separately as directly or indirectly assigned.	275192
The button for deleting an attestation polices is now grayed out as long as any attestation cases associated with it still exist.	275625

Resolved issues

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

Table 8: Starling CertAccess Agent

Resolved issue	Issue ID
If an error occurs when provisioning memberships in Active Directory groups, the provisioning process is never completed.	34489
After uninstalling the Starling CertAccess Agent, an incorrect message is displayed in the Uninstall Wizard.	34515, 279102
Email notifications about granted request approvals name the wrong approver.	34614
No more email notifications are sent about pending attestation requests.	34661

Table 9: Starling CertAccess Web Portal

Resolved issue	Issue ID
If a processing time > 0 is given for an attestation policy, sometimes no due date is set for the attestation case.	34546
Error in the Web Portal when starting attestation if the **Attestation Policies** page is already open but has not been used for a while.	279980
Error if products in the shopping cart are requested for multiple identities.	283037

List of resolved issues in previous versions of Starling CertAccess

Resolved issues in the version from August 26, 2021

Table 10: General

Resolved issue	Issue ID
Error validating the access token on the application server.	34485, 282235
Error in the Starling CertAccess Service when updating the access token: `There was an error retrieving an access token: BadRequest - Bad Request.`	34486, 282245

Table 11: Starling CertAccess Agent

Resolved issue	Issue ID
In a demo test environment, the email settings are not set.	34405
After an initial synchronization, the identities are not always created.	34408, 278859
Synchronization stopped due to an error synchronizing with revision filtering: The revision property type does not match. Error message: `Error filtering by revision. ---> System.ArgumentException: Object must be of type Int32.`	34462
When automatically assigning identities to user accounts, an account manager already assigned to the user accounts (`ADSAccount.ObjectKeyManager`) is removed again.	34464
The administrative user's password must not expire.	34468
After synchronization, a display name is automatically given to Active Directory groups with a missing display name. This triggers unwanted provisioning.	34469
The sender's email address cannot be edited in the Starling CertAccess Launchpad.	281018

Table 12: Starling CertAccess Web Portal

Resolved issue	Issue ID
Users of the demo test environment do not receive email notifications.	34402, 279389
When attestation cases are created on a scheduled basis, the attestation history does not contain entries with the **Created** status.	34426
Incorrect approvals are stored in the attestation history if an attestation case has been processed more than once.	34427
When viewing memberships in system entitlements in the Data Explorer, the navigation buttons do not work.	277431
Missing handling of NULL values.	277875

Resolved issues in the version from May 5, 2021

Table 13: Starling CertAccess Agent

Resolved issue	Issue ID
In the Launchpad, the help does not work in the **Starling CertAccess configuration data** dialog.	34207, 274123
Error occurs if several queries with the same access token reach the application server at the same time.	34220, 270570, 274597
Error generating reports if the query contains an order by statement.	34240

Table 14: Starling CertAccess Web Portal

Resolved issue	Issue ID
In reports, the user who added an assignment is not always displayed.	34093
Missing page break in the **Risk index (calculated)** column heading in some reports.	34259
In the web browser, query exceptions appear as errors in the log files.	271770
When you log off from the Web Portal and log in again with another user, the user profile is displayed incorrectly.	271824

Known issues

The following is a list of issues known to exist at the time of release of Starling CertAccess.

- There are no known issues for this release.

System requirements

Before using the October 7, 2021 Starling CertAccess release, ensure that your system meets the following minimum system requirements.

Supported browsers

You can use any browser to access Starling CertAccess if it is supported by One Identity Starling. For more information about this, see the *One Identity Starling User Guide*.

> NOTE: Starting February 1, 2022, One Identity Starling will no longer support Internet Explorer 11.

Enable JavaScript in your browser for the Starling CertAccess Web Portal to work. A minimum screen resolution of 1280x1024 pixels is recommended with at least 16-bit color in order to optimize the user interface graphics. A display size of at least 9.7 inches is recommended for mobile displays, for example, when using a tablet.

Starling CertAccess Agent system requirements

The following system requirements represent the minimum requirements for installing and unlimited operation of the Starling CertAccess Agent. You install the Starling CertAccess Agent on an administrative workstation. You install the Starling CertAccess Service on a server. On the server, the Active Roles ADSI client for communicating with Active Roles must be installed respective to the version of Active Roles. A server running the Starling CertAccess Service will be subsequently named the Job server. For detailed information about the system requirements, see the *One Identity Starling CertAccess Administration Guide for One Identity Active Roles Integration*.

Every Starling CertAccess Agent installation can be virtualized. Ensure that performance and resources are available to the respective Starling CertAccess Agent component according to system requirements. Virtualization of a Starling CertAccess Agent installation should only be attempted by experts with strong knowledge of virtualization techniques.

> NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

Table 15: Minimum system requirements - Job server

Processor	8 physical cores 2.5 GHz+

Memory	16 GB RAM
Hard drive storage	40 GB
operating system	Windows operating systems Following versions are supported: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012
Additional software	• Microsoft .NET Framework Version 4.7.2 or later NOTE: Take the target system manufacturer's recommendations for connecting the target system into account. • One Identity Active Roles Management Shell for Active Directory (x64) On 32-bit operating systems, use the Active Roles Management Shell for Active Directory (x86) package. For installation instructions, refer to your *One Identity Active Roles documentation*. • The following packages must be subsequently installed from the Active Roles installation medium: On 32-bit systems: • `<source>\Redistributables\vc_redist.x86.exe` • `<source>\Components\ActiveRoles ADSI Provider\ADSI_x86.msi` On 64-bit systems: • `<source>\Redistributables\vc_redist.x64.exe` • `<source>\Components\ActiveRoles ADSI Provider\ADSI_x64.msi` Furthermore, it is necessary that connections can be established from the Job server to the Active Roles server over the **15172** port. If necessary, a firewall rule must be set up on the Active Roles server.

Table 16: Minimum system requirements - administrative workstations

Processor	4 physical cores 2.5 GHz+
Memory	4 GB+ RAM
Hard drive storage	1 GB

operating system	Windows operating systems Following versions are supported: • Windows 10 (32-bit or 64-bit) with version 1511 or later • Windows 8.1 (32-bit or 64-bit) with the current service pack
Additional software	• Microsoft .NET Framework Version 4.7.2 or later • Microsoft Edge WebView2 • Active Roles ADSI Provider of the Active Roles version to be connected To set up synchronization with a Active Directory domain, it must be possible to establish a connection to the Active Roles server using the port **15172** (TCP). If necessary, a firewall rule must be set up on the Active Roles server.
Supported browsers	• Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Table 17: Supported data systems

Active Roles connector	Active Roles 7.4.1, 7.4.3, and 7.4.4

Product licensing

Use of this software is governed by the Software Transaction Agreement found at http://www.oneidentity.com/legal/sta.aspx and the SaaS Addendum at http://www.oneidentity.com/legal/saas-addendum.aspx. This software requires an activation or license key to operate.

Additional resources

Additional information is available in:

- Starling CertAccess Support
- Starling CertAccess Online documentation
- Starling Online Community

Globalization

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

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

The release is localized in the following languages: German

About us

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

Contacting us

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

Technical support resources

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

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

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

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. 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.**