One Identity Starling CertAccess

Administration Guide for One Identity Active Roles Integration

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.

Starling CertAccess Administration Guide for One Identity Active Roles Integration
Updated - 21 September 2022, 15:26

Contents

About this guide

One Identity Starling CertAccess integrates One Identity Active Roles and One Identity Manager in the Starling CertAccess cloud-based service. You use the Starling CertAccess Agent to set up synchronization between an Active Directory environment managed by One Identity Active Roles and Starling CertAccess.

The *One Identity Starling CertAccess Administration Guide for One Identity Active Roles Integration* describes how you provide Starling CertAccess to your company. It includes installing and working with the Starling CertAccess Agent. You will discover, which prerequisites you require for the installation and how to use the Starling CertAccess Agent components.

The *One Identity Starling CertAccess Administration Guide for One Identity Active Roles Integration* is aimed at Active Roles administrators that utilize Starling CertAccess to help manage Active Directory through One Identity Active Roles, allowing you to handle access requests and carry out access certifications.

For more information about how to handle access requests and carry out access certifications, see the *One Identity Starling CertAccess Web Portal User Guide*.

The *One Identity Starling CertAccess Operations Support Web Portal User Guide* explains how to monitor process handling, check the synchronization status of connected target systems, and identify failed processes.

Available documentation

The online version of Starling CertAccess documentation is available in the Support portal under Starling CertAccess online documentation.

Starling CertAccess basics

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.

Use **Starling CertAccess Agent** to set up synchronization between a One Identity Active Roles managed Active Directory and Starling CertAccess. Synchronization transfers all the required data for controlling access, such as user accounts, groups, and group memberships.

Users can use **Starling CertAccess Web Portal** to request memberships in Active Directory groups (access request). Managers and others responsible for compliance can certify the correctness of access requests as well as recertify existing memberships using regular attestation (access certification). All memberships are assigned to specific identities allowing access permissions to be tested to see if they are valid in that combination. This ensures that regulatory requirements are fulfilled. If, during attestation, certain access permissions are identified as being invalid and certification is therefore denied, the affected memberships are automatically deleted. Changes such as authorized access requests or revoked access permissions are immediately provisioned in the connected Active Directory domains and take effect straightaway.

The Starling CertAccess Web Portal provides various reports containing information about synchronized data, available access permissions, or completed attestations. You can use these reports for analyzing and summarizing important information.

The **Starling CertAccess Operations Support Web Portal** helps you to run your Starling CertAccess instance. For example, you can monitor the process handling, identify failed processes, take measures and re-run the processes, view the synchronization status and synchronization logs.

Starling CertAccess is integrated as a Starling service in One Identity Starling (https://cloud.oneidentity.com). You can subscribe to a trial version of the Starling service, filled with sample data, to help you understand the functionality better before you commit to a paid subscription. The One Identity sales team will support you if you wish to carry out a Proof of Concept trial with your own data.

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*.

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.

Additional hardware and software prerequisites

The hardware and software prerequisites for One Identity Starling apply to Starling CertAccess. The prerequisite for registering and signing in to One Identity Starling is an Azure Active Directory tenant. Use your Azure Active Directory credentials to register. For more information about this, see the *One Identity Starling User Guide*.

Using Starling CertAccess as a Starling service

To use Starling CertAccess as a Starling service, you require a Starling organization. You can add the Starling service to an existing organization or set up a new one. For more information about organizations, see the *One Identity Starling User Guide*.

Once you have created a Starling organization, you can add Starling CertAccess as a Starling service to it. You can select the following subscription types for Starling CertAccess:

- Paid subscriptions on page 10
- Trial subscriptions on page 7

Trial subscriptions

Starling CertAccess can be subscribed for a limited period to test the product before you make a longer term commitment to using it. If you decide not to upgrade your subscription, Starling CertAccess will no longer be accessible.

You can trial Starling CertAccess in two ways.

1. If you want to see how the main functions of Starling CertAccess work, start a Demo Trial. With this, you can try out all the functions using a standard set of sample data, without needing to connect Starling CertAccess to your own One Identity Active Roles installation. A Demo Trial is time-limited to five days, but if you need more time, you can start your trial again before the trial subscription ends.
2. If you want to go a step further and try Starling CertAccess with your own One Identity Active Roles installation, then you can request a Proof of Concept trial. This will allow you to trial Starling CertAccess Web Portal functions and also let you see how data is synchronized between your own Active Roles and Starling CertAccess. You will see the product performing exactly how it would with a fully-paid subscription with no restrictions. For a Proof of Concept Trial, install all the local components on a workstation within your system.

   A Proof of Concept Trial is limited to 14 days but if you need more time, you can start your Proof of Concept Trial again before the trial subscription ends.

   To acquire a Proof of Concept Trial license, contact One Identity sales.

A trial subscription is limited to 30 days. Within this time period, you can start and end Demo and Proof of Concept trials as often as you wish. If the demo period for the trial subscription has expired but you still require more time for testing, you can extend the trial period once-off for another 30 days. To do this, contact One Identity sales.

Detailed information about this topic

- Starting a trial subscription on page 8
- Ending a trial subscription on page 9

Related topics

- Paid subscriptions on page 10
- Using Starling CertAccess as a Starling service on page 7

Starting a trial subscription

Once you have registered with One Identity Starling you can trial the Starling Service Starling CertAccess.

To start a trial subscription

1. Sign in to Starling.
2. On the home page, select Starling Service **Starling CertAccess** and click **Trial**.
3. In the **Your Location** dialog, select your country and state or province.

   This dialog only appears the first time you trial a service after you have added Starling CertAccess to your organization.

4. Click **Confirm**.
5. Enter a domain name for your Starling CertAccess trial instance.

   The domain name may not be longer than 40 characters and must be unique within Starling.
6. To start a trial demo, click **Demo trial**.

   - OR -

   To start a proof of concept trial, click **Proof of concept trial**.
7. This starts up a trial instance.

   It can take a while to complete. Once your trial instance is ready to use, you will receive a confirmation email with a link.
8. If you have started a proof of concept trial, you now install the Starling CertAccess Agent and set up synchronization with your One Identity Active Roles.

   For more information, see Setting up the initial synchronization with Active Roles on page 16.
9. If you have started a Demo trial, on the Starling CertAccess website, click **Go**.

   This opens the Starling CertAccess Web Portal.

Starling CertAccess is shown as a new tile on the Starling home page in the **My Services** section and can be used until trial period ends. The number of days remaining in your trial are indicated by a countdown on the tile. You can purchase a paid subscription at any time during the trial period. Click **More Information** on the Starling CertAccess tile to find out how you can purchase the product.

Related topics

- Ending a trial subscription on page 9
- Paid subscriptions on page 10

Ending a trial subscription

A trial subscription is limited to 30 days. Within this time period, you can start and end Demo and Proof of Concept trials as often as you wish. Once the demo period has expired, the service will no longer be accessible. When you purchase a paid subscription or you want to start a new trial, you can end your current trial early.

To end a trial subscription early

1. In the **Trial Details** section on the Starling CertAccess website, click the **End Trial** button.
2. Click **OK**.

Related topics

- Starting a trial subscription on page 8
- Paid subscriptions on page 10

Paid subscriptions

You can purchase a Starling CertAccess subscription through any Starling organization. A paid subscription offers you full access to the product (including the Starling CertAccess Agent) for the length of your contract and with a fixed number of user licenses. You will find pricing information about subscriptions for Starling CertAccess as a Starling Service on the Starling home page by clicking the **More Information** button. For more information, see Starling a paid subscription on page 10.

NOTE: To end your paid subscription, contact One Identity sales or support.

Related topics

- Trial subscriptions on page 7
- Using Starling CertAccess as a Starling service on page 7

Starting a paid subscription

To start a paid subscription, register with One Identity Starling and contact sales.

To start a paid subscription

1. Sign in to Starling.
2. On the home page, select the Starling Service **Starling CertAccess** and contact sales.

   Once the subscription has been set up and your Starling CertAccess instance has been provisioned, you will receive an email.
3. If your trial period has not expired yet, end the trial.

   For more information, see Ending a trial subscription on page 9.
4. Enter a domain name for your productive Starling CertAccess instance.

   The domain name may not be longer than 40 characters and must be unique within Starling.
5. Click **Production**.
6. This starts up a Starling CertAccess instance.

   It can take a while to complete. Once the instance is ready to use, you will receive an email containing a link to your instance.

The instance is set up completely new. Data that were synchronized during the trial phase are no longer available.

7. Install the Starling CertAccess Agent and set up your One Identity Active Roles synchronization.

   For more information, see Setting up the initial synchronization with Active Roles on page 16.

Related topics

- Paid subscriptions on page 10

Updating the Starling CertAccess instance

From time to time, your Starling CertAccess instance may not be available due to maintenance work. Your Starling administrator is notified about the upcoming maintenance work. Administrative users see a warning on the Starling CertAccess website. If the instance is not accessible, all users see an appropriate message.

Related topics

- Updating the Starling CertAccess Agent on page 28

Handling processes in Starling CertAccess

Starling CertAccess Agent uses so called 'processes' for mapping business processes. A process consists of process steps, which represent processing tasks and are joined by predecessor/successor relations. For example, a process might control how user accounts are created that are transferred to your Starling CertAccess instance by synchronization. Individual process steps create the user accounts and assign identities.

Processes in the Frozen status

In the Starling CertAccess Operations Support Web Portal you can monitor the runtime status. Each process step of the processes that are currently running is flagged with the current runtime status. Process steps with the **Frozen** runtime status require special attention. Here, errors have occurred during processing, which you must check and correct in each individual case. Subsequently, these process steps can be reactivated and re-processed.

Unresolved references

When synchronizing a target system environment, object references might not be resolved. This occurs when the referenced objects do not exist in your Starling CertAccess instance. These unresolved references are written to a data store. This ensures that the references remain intact and are not deleted by target system provisioning. In the Operations Support Web Portal, you can see an overview of the unresolved references. You can check each one of them and correct them in the connected target system.

Regular checking with the Operations Support Web Portal

Errors may occur during synchronization as well as during processing, which may lead to inconsistent or incorrect data in your Starling CertAccess instance or in the connected target system. Therefore, use the Operations Support Web Portal regularly to:

- Monitor the overview of processes with the **Frozen** status
- View synchronization logs
- Check unresolved references

Make the necessary corrections.

For more information about this, see the *One Identity Starling CertAccess Operations Support Web Portal User Guide*.

3

The Starling CertAccess Agent architecture

The Starling CertAccess Agent secures the data exchange between Starling CertAccess and Active Directory managed through One Identity Active Roles. The Starling CertAccess Agent synchronizes the Active Directory environment and immediately provisions changes that were made in Starling CertAccess in the connected Active Directory domains. Synchronization is started once a day.

The Starling CertAccess Agent contains on-premises components that are required for the Starling CertAccess configuration and for synchronizing with One Identity Active Roles.

The Starling CertAccess Agent consists of the following components:

- **Starling CertAccess Launchpad**

  Use the Starling CertAccess Launchpad to guide you through various administrative tasks:

  - Manage Starling CertAccess administrators
  - Install the Starling CertAccess Service
  - Configure email notification distribution
  - Install the Active Roles ADSI provider
  - Set up synchronization and synchronize an Active Directory environment through One Identity Active Roles
  - Display the Starling CertAccess Service's status
  - Configure automatic identity assignment
  - Configure automatic assignment of system entitlements to the IT Shop

  You install the Starling CertAccess Launchpad on an administrative workstation.

- **Starling CertAccess Service**

  The Starling CertAccess Service carries out the following tasks:

  - Synchronization between Starling CertAccess and Active Roles
  - Distribution of email notifications
  - Generating reports

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 is subsequently called the Job server.

Starling CertAccess Agent supports synchronization with Active Roles versions 7.4.1, 7.4.3 and 7.4.4.

Figure 1: The Starling CertAccess Agent architecture

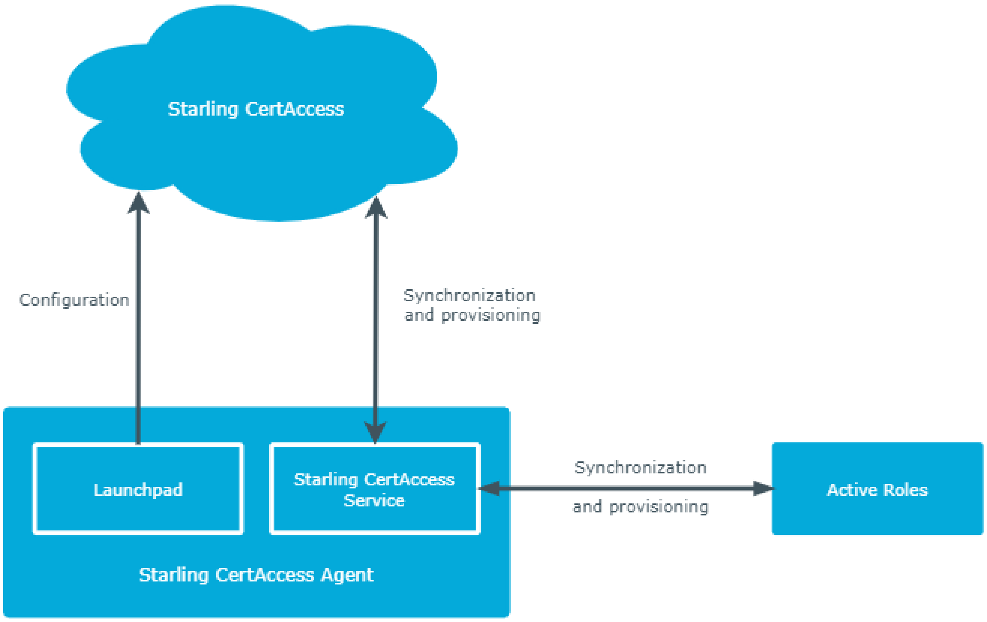
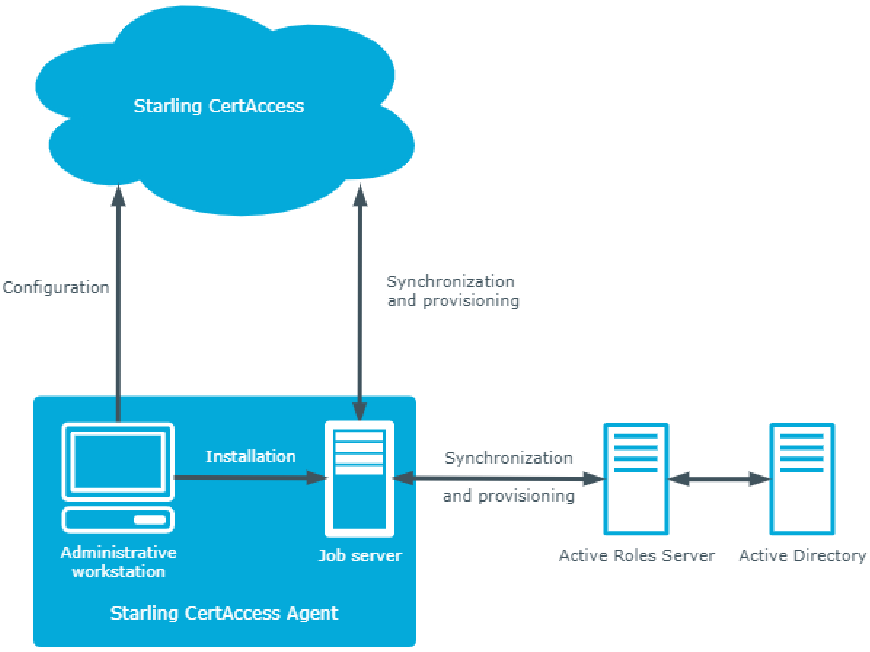

Starling CertAccess
Configuration
Synchronization and provisioning
Launchpad
Starling CertAccess Service
Synchronization
and provisioning
Active Roles
Starling CertAccess Agent

Figure 2: Starling CertAccess Agent topology



Related topics

- Handling processes in Starling CertAccess on page 11

Setting up the initial synchronization with Active Roles

Once you have prepared Starling CertAccess for your organization, you can set up initial synchronization with your One Identity Active Roles. For this, you install the Starling CertAccess Agent on an administrative workstation. Use the Starling CertAccess Launchpad to install the Starling CertAccess Service on a Job server.

Ensure that all the system requirements on the workstation and the Job server are fulfilled. For more information, see Starling CertAccess Agent system requirements on page 21.

To set up synchronization with Active Roles

1. In the **Subscription is ready** email, click the **Get Started** button.

   This opens the Starling CertAccess website.

2. Download the Starling CertAccess Agent installation package onto a workstation.
   1. Under **Step 1**, click **Download Agent**.
   2. Copy the Starling CertAccess Agent key into the clipboard. Under **Step 2**, click **Copy**.

      > IMPORTANT: Save your Starling CertAccess Agent key in a safe place because you will need it later.

3. Install the Starling CertAccess Agent on the workstation.
   1. Unpack the Starling CertAccess Agent installation package in a temporary directory on the administrative workstation.
   2. Start the `autorun.exe` file from the temporary directory.

      This starts the installation wizard.
   3. On the start page, select the language for the installation wizard.
   4. Confirm the conditions of the license.
   5. On the **Installation settings** page, enter the following information.
      - **Installation source**: Select the temporary directory containing the installation files.

- **Installation directory**: Select the directory in which you want to install the files for the Starling CertAccess Agent.

  > NOTE: To make additional changes to the configuration settings, click on the arrow button next to the input field. Here, you can specify whether you are installing on a 64-bit or a 32-bit operating system.
  >
  > For a standard installation, no further configuration settings are necessary.

f. On the **Install WebView2** page you are prompted to install Microsoft Edge WebView2. The user interface of some Starling CertAccess Agent components requires Microsoft Edge WebView2 to display certain content.

> NOTE: This page is only shown if you want to install Starling CertAccess Agent components that are expecting WebView2 and WebView2 is not yet installed.

g. On the last page of the installation wizard, click **Start** to run the Starling CertAccess Launchpad.

When you start the Launchpad for the first time, enter the Starling CertAccess Agent key data for your Starling CertAccess instance.

i. In the **Starling CertAccess configuration data** dialog, copy your Starling CertAccess Agent key into the text field.

ii. Click **OK**.

h. Click **Finish** to close the installation wizard.

4. The first time you start the Launchpad, the Starling CertAccess Agent is updated automatically. This loads the newest version of the Starling CertAccess Agent and installs it.
   - Click **Yes**.
5. Sign in with your Starling credentials.
   - Click **Next**.

     This starts the Launchpad.
6. Install the Starling CertAccess Service.

   The Starling CertAccess Service is installed remotely on a Job server.

   Prerequisites:

   - The server fulfills the minimum system requirements. For more information, see Minimum system requirements for the Job server on page 22.

   a. In the Launchpad, select **Administrative tasks > System configuration > Install service**.

   b. Click **Run**.

   c. On the Server Installer start page, click **Next**.

   d. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.

   e. On the **Service access** page, enter the service's installation data.

      - **Computer**: Enter the name or IP address of the server that the service is installed and started on.

      - **Service account**: Enter the details of the user account that the Starling CertAccess Service is running under. Enter the user account, the user account's password and password confirmation.

      The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the Starling CertAccess Service details, such as the installation directory, name, display name, and the Starling CertAccess Service description, using the advanced options.

   f. Click **Next** to start installing the service.

      Installation of the service occurs automatically and may take some time.

   g. Click **Finish** on the last page of the Server Installer.

      > NOTE: In a default installation, the service is entered in the server’s service management with the name **Starling CertAccess Service**.

7. Install the Active Roles ADSI provider.

   a. In the Launchpad, select **Administrative tasks > Data synchronization > Install Active Roles ADSI Provider**.

   b. Click **Install**.

   c. Use the file explorer to select the path to the `ActiveRoles.exe` file. Select the file and click **Open**.

      This runs the installation.

      Once installing is complete, the **Install** button is grayed out in the Launchpad.

8. Set up synchronization with Active Roles.

   a. In the Launchpad, select **Administrative tasks > Data synchronization > Configure Active Roles synchronization**.

   b. Click **Run**.

      This starts the system connection wizard.

   c. On the start page of the system connection wizard, click **Next**.

   d. On the **Target server** page, enter the Active Roles server to which you want to connect. If possible, servers are determined automatically.

- In the **Host name/IP address** menu, select a target server.
- If the server cannot be found automatically, in the **Host name/IP address** field, enter the DNS name or the IP address.

e. On the **Credentials** page, enter the user account and password for accessing Active Roles.

f. On the **Domain/root entry selection** page, select the domain you want to synchronize or enter the root entry's distinguished name.

g. On the last page of the system connection wizard, click **Finished**.

Synchronization is now set up.

The Launchpad shows the **Manage synchronization** task.

9. Start the synchronization.

a. In the Launchpad, select **Administrative tasks > Data synchronization > Manage synchronizations**.

b. Click **Run**.

c. In the **Maintain synchronizations** dialog, select the domain.

d. Click **Start synchronization**.

e. Confirm the security prompt with **Yes**.

f. Close the alert with **OK**.

The **Manage synchronization** dialog displays the current status of the synchronization.

> TIP: You can display the Starling CertAccess Service log in a browser. The log file shows you the synchronization's progress. Here you can check that the Starling CertAccess Service is working correctly.
>
> For more information, see Displaying the Starling CertAccess Service log file on page 46.

If synchronization is complete, you will see the synchronized data in the Starling CertAccess Web Portal.

10. Check that the data has been synchronized correctly.

a. Switch to the Starling CertAccess website and click **Go**.

This opens the Starling CertAccess Web Portal.

b. Select the **Data > Data Explorer** menu.

c. In the Data Explorer's navigation, click **Identities**, **User accounts**, and **System entitlements** one after another to check the integrity of the data.

For more information about the Starling CertAccess Web Portal, see *One Identity Starling CertAccess Web Portal User Guide*.

Detailed information about this topic

- The Starling CertAccess Agent architecture on page 13
- Installing the Starling CertAccess Agent on a workstation on page 27
- Installing the Starling CertAccess Service on page 35
- Minimum system requirements for the Job server on page 22
- Permissions required for synchronizing with One Identity Active Roles on page 25
- Installing the Active Roles ADSI provider on page 42
- Setting up synchronization with an Active Directory domain on page 42
- Mapping Active Roles schema types in Starling CertAccess on page 51

Starling CertAccess Agent system requirements

Starling CertAccess Agent supports synchronization with Active Roles versions 7.4.1, 7.4.3 and 7.4.4. The system requirements described here represent the minimum requirements for unlimited operation and usage of the Starling CertAccess Agent.

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. For more information about virtual environments, see Product Support Policies.

Detailed information about this topic

Minimum system requirements for administrative workstations

The Starling CertAccess Agent is installed on an administrative workstation to edit and display data. To do this, the following system prerequisites must be guaranteed:

Table 1: Minimum system requirements - administrative workstations

Processor	4 physical cores 2 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) minimum version 1511 - 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)

Minimum system requirements for the Job server

The following system prerequisites must be fulfilled to install the Starling CertAccess Service on a server.

Table 2: 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 The 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: When connecting the target system, refer to the target system manufacturer's recommendations. • 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.

To remotely install the Starling CertAccess Service, you must have an administrative workstation on which the Starling CertAccess Agent components are installed.

Related topics

- Installing the Starling CertAccess Service on page 35
- Minimum system requirements for administrative workstations on page 21

Setting up permissions for creating an HTTP server

The log files of the Starling CertAccess Service can be displayed using an HTTP server (http://<server name>:<port number>).

Users require permission to open an HTTP server. The administrator must grant URL approval to the user to do this. This can be run with the following command line call:

```
netsh http add urlacl url=http://*:<port number>/ user=<domain>\<user name>
```

If the Starling CertAccess Service has to run under the Network Service's user account (**NT Authority\NetworkService**), explicit permissions for the internal web service must be granted. This can be run with the following command line call:

```
netsh http add urlacl url=http://<IP address>:<port number>/ user="NT
AUTHORITY\NETWORKSERVICE"
```

You can check the result with the following command line call:

```
netsh http show urlacl
```

Communications ports and firewall configuration

Starling CertAccess Agent is made up of several components that can run in different network segments. In addition, Starling CertAccess Agent requires access to various network services, which can also be installed in different network segments. You must open various ports depending on which components and services you want to install behind the firewall.

The following ports are required:

Table 3: Communications port

Default port	Description
1433	Port for communicating with Starling CertAccess.
1880	Port for the HTTP protocol of Starling CertAccess Service.
88	Kerberos authentication system (if Kerberos authentication is implemented).
135	Microsoft End Point Mapper (EPMAP) (also, DCE/RPC Locator Service).
137	NetBIOS Name Service.
139	NetBIOS Session Service.

Starling CertAccess Agent users

Users with the following permissions are used for working with the Starling CertAccess Agent and for synchronizing with Active Roles:

Table 4: Starling CertAccess Agent users

User	Entitlements
User for logging into the Starling CertAccess Agent	By default, the user that you used to initially register for One Identity Starling has administrative permissions for Starling CertAccess and the Starling CertAccess Agent. This user can grant other administrative users access to Starling CertAccess. Users that login to the Starling CertAccess Launchpad are authenticated with OAuth 2.0.
User account for the Starling CertAccess Service	The user account for the Starling CertAccess Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires permissions for the internal web service. NOTE: If the Starling CertAccess Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the Starling CertAccess Service installation directory in order to automatically update Starling CertAccess Agent. In the default installation, Starling CertAccess Agent is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)

Related topics

- Managing Starling CertAccess administrators on page 34

Permissions required for synchronizing with One Identity Active Roles

It is recommended to set up a separate user account to use for connecting to Active Directory through for Active Roles. Use Active Roles Access Templates for the configuration. By using access templates, you delegate administration-relevant permissions to an Active Directory user account but without issuing the permissions directly in Active Directory. For more information about Active Roles Access Templates, see your *One Identity Active Roles documentation*.

The following Access Templates are suggested for delegating permissions:

- All Objects - Read All Properties
- All Objects - Full Control

Starling CertAccess Agent works without controlling Active Roles workflows. To avoid any existing Active Roles workflows, you must add the user account to the **Active Roles administrators** group.

Edit the Active Roles admins in the Active Roles Configuration Center. If a user account is entered in the Active Roles Configuration Center as an Active Roles Admin, this is the user account that must be used. For more information about editing the group or the user account for administrative access, see your *One Identity Active Roles documentation*.

6

Installing, updating, and uninstalling Starling CertAccess Agent components

To be able to work with Starling CertAccess, install the Starling CertAccess Agent components on an administrative workstation and on a server. Install the following components:

- Workstation: Starling CertAccess Launchpad
- Server: Starling CertAccess Service

All components are automatically updated when your Starling CertAccess instance is updated. To uninstall the components, use the Windows standard functionality for uninstalling programs on the workstation and the server.

Detailed information about this topic

- Installing the Starling CertAccess Agent on a workstation on page 27
- Installing the Starling CertAccess Service on page 35
- Updating the Starling CertAccess Agent on page 28
- Uninstalling the Starling CertAccess Agent on page 29

Installing the Starling CertAccess Agent on a workstation

You install the Starling CertAccess Agent on an administrative workstation. An installation wizard helps you with the Starling CertAccess Agent installation.

> IMPORTANT: Before you begin the installation, ensure that the workstation fulfills all the system requirements. For more information, see Starling CertAccess Agent system requirements on page 21.

To install the Starling CertAccess Agent

1. Unpack the Starling CertAccess Agent installation package in a temporary directory on the administrative workstation.
2. Start the `autorun.exe` file from the temporary directory.

   This starts the installation wizard.
3. On the start page, select the language for the installation wizard.
4. Confirm the conditions of the license.
5. On the **Installation settings** page, enter the following information.
   - **Installation source**: Select the temporary directory containing the installation files.
   - **Installation directory**: Select the directory in which you want to install the files for the Starling CertAccess Agent.

     > NOTE: To make additional changes to the configuration settings, click on the arrow button next to the input field. Here, you can specify whether you are installing on a 64-bit or a 32-bit operating system.
     >
     > For a standard installation, no further configuration settings are necessary.
6. On the **Install WebView2** page you are prompted to install Microsoft Edge WebView2. The user interface of some Starling CertAccess Agent components requires Microsoft Edge WebView2 to display certain content.

   > NOTE: This page is only shown if you want to install Starling CertAccess Agent components that are expecting WebView2 and WebView2 is not yet installed.
7. On the last page of the installation wizard, click **Start** to run the Starling CertAccess Launchpad.
8. Click **Finish** to close the installation wizard.

The Starling CertAccess Agent is installed for all user accounts on the workstation. In the default installation, Starling CertAccess Agent is installed under:

- `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems)
- `%ProgramFiles%\One Identity` (on 64-bit operating systems)

Related topics

- Working with the Starling CertAccess Agent on page 31
- Starting the Starling CertAccess Launchpad on page 32
- Updating the Starling CertAccess Agent on page 28

Updating the Starling CertAccess Agent

If your Starling CertAccess instance has been update, the Starling CertAccess Agent updates automatically the next time the Launchpad starts. This loads the newest version of the Starling CertAccess Agent and installs it. Starling CertAccess Agent components are also updated automatically on the Job server.

Related topics

- Starting the Starling CertAccess Launchpad on page 32
- Updating the Starling CertAccess instance on page 11

Uninstalling the Starling CertAccess Agent

To uninstall the Starling CertAccess Agent, remove the Starling CertAccess Agent components from the administrative workstation and from the server running the Starling CertAccess Service (Job server). To do this, use the Windows standard functionality for uninstalling programs.

To remove the Starling CertAccess Agent from the workstation

1. Start uninstalling the Starling CertAccess Agent using Windows standard functionality for uninstalling programs.

   This starts the Starling CertAccess uninstall wizard.
2. On the start page, select the language for the wizard and click **Next**.
3. The **Uninstall** page shows the directory from which the Starling CertAccess Agent components will be removed.
   a. (Optional) To remove log files and configuration data as well (for example, registry entries), enable **Remove all configuration data and log files**.

      As long as there are more that one Starling CertAccess Agent installations on the workstation, the configuration data cannot be removed.
   b. Click **Next**.
   c. Confirm the security prompt with **OK**.
4. Click **End** on the last page to end the program.

To remove the Starling CertAccess Agent from the Job server

1. Start the Services manager on the Job server and end the **Starling CertAccess Service**.
2. Start uninstalling the Starling CertAccess Agent using Windows standard functionality for uninstalling programs.

   This starts the Starling CertAccess uninstall wizard.
3. On the start page, select the language for the wizard and click **Next**.

4. The **Uninstall** page shows the directory from which the Starling CertAccess Agent components will be removed.
    a. To remove log files and configuration data as well (for example, registry entries), enable **Remove all configuration data and log files**.
    b. Click **Next**.
    c. Confirm the security prompt with **OK**.
5. Click **End** on the last page to end the program.

Related topics

- Installing the Starling CertAccess Agent on a workstation on page 27
- Updating the Starling CertAccess Agent on page 28
- Installing the Starling CertAccess Service on page 35

7

Working with the Starling CertAccess Agent

Use the Starling CertAccess Agent to set up synchronization between an Active Roles managed Active Directory environment and Starling CertAccess. In this case, the Active Directory domains are seen as the primary system. Modifications in the primary system are transferred on a daily basis to Starling CertAccess. Changes to Active Directory group memberships in Starling CertAccess are published immediately in the Active Directory domain.

Use the Starling CertAccess Agent to perform the following:

- Manage Starling CertAccess administrators
- Install the Starling CertAccess Service
- Configure email notification distribution
- Install the Active Roles ADSI provider
- Set up synchronization and synchronize an Active Directory environment through One Identity Active Roles
- Display the Starling CertAccess Service's status
- Configure automatic identity assignment
- Configure automatic assignment of system entitlements to the IT Shop

TIP: To open the themed help, click ? for the respective task.

Detailed information about this topic

- Starting the Starling CertAccess Launchpad on page 32
- Managing Starling CertAccess administrators on page 34
- Installing the Starling CertAccess Service on page 35
- Configuring automatic assignment of identities on page 40
- Configuring automatic IT Shop assignment on page 41
- Installing the Active Roles ADSI provider on page 42
- Setting up synchronization with an Active Directory domain on page 42

- Synchronization maintenance on page 44
- Displaying the Starling CertAccess Service log file on page 46

Starting the Starling CertAccess Launchpad

The Starling CertAccess Launchpad allows you to run all the functions of the Starling CertAccess Agent.

To start the Launchpad

1. In the Windows start menu, select **Starling CertAccess Launchpad**.
2. When prompted, enter the configuration data for your Starling CertAccess instance.
    a. In the **Starling CertAccess configuration data** dialog, copy your Starling CertAccess Agent key into the text field.
    b. Click **OK**.
3. If your Starling CertAccess instance has been updated, the Starling CertAccess Agent updates automatically as well. This loads the newest version of the Starling CertAccess Agent and installs it.
    - In the **Auto update** prompt, click **Yes**.
4. Sign in with your Starling credentials.
    - Click **Next**.

      This starts the Launchpad.
5. To minimize the application in the task bar, click **Close**.

Related topics

- Working with the Starling CertAccess Agent on page 31
- Loading the Starling CertAccess instance configuration file on page 32
- Updating the Starling CertAccess instance on page 11

Loading the Starling CertAccess instance configuration file

To communicate with Starling CertAccess, the Starling CertAccess Agent requires the key of your Starling CertAccess instance. This key might be required when you start the

Launchpad for the first time or when you set up synchronization. The key is not stored permanently due to security reasons and must be renewed when required.

To use the Starling CertAccess Agent key

1. Open your Starling CertAccess instance's Starling CertAccess website.
2. Copy the Starling CertAccess Agent key into the clipboard. Under **Step 2**, click **Copy**.

   > IMPORTANT: Save your Starling CertAccess Agent key in a safe place because you will need it later.

To load the configuration data

1. In the **Starling CertAccess configuration data** dialog, copy your Starling CertAccess Agent key into the text field.
2. Click **OK**.

Related topics

- Setting up the initial synchronization with Active Roles on page 16
- Working with the Starling CertAccess Agent on page 31
- Starting the Starling CertAccess Launchpad on page 32
- Installing the Starling CertAccess Service on page 35
- Setting up synchronization with an Active Directory domain on page 42

Editing general settings

The initial Launchpad login uses the system language for the user interface. In the Launchpad's general settings, you can change the language

To change the general settings

1. In the Launchpad's header, click ⌄.
2. Select **Settings**.
3. Edit the following settings.
   - **Language**: Language used for formatting data, such as date formats, time formats, and number formats.
   - **Alternative display language**: This specifies whether the Starling CertAccess Agent's application text is displayed in another language. The language changes take effect after restarting the Launchpad.
4. Click **OK**.
5. Restart the Launchpad.

Related topics

- Starting the Starling CertAccess Launchpad on page 32

Managing Starling CertAccess administrators

By default, the user that you used to initially register for One Identity Starling has administrative permissions for Starling CertAccess and the Starling CertAccess Agent. This user can grant other administrative users access to Starling CertAccess.

Starling CertAccess administrators configure Starling CertAccess using the Launchpad, they are target system managers for Active Directory, manage users, configure attestation and the IT Shop for requests.

To add an administrative user

1. In the Launchpad, select **Administrative tasks > System configuration > Manage administrators**.
2. Click **Run**.

   This opens the **Manage Starling CertAccess administrators** dialog.
3. Click **New**.
4. Enter the email address of the additional user.
5. Click **OK**.

To edit an administrative user

1. In the Launchpad, select **Administrative tasks > System configuration > Manage administrators**.
2. Click **Run**.

   This opens the **Manage Starling CertAccess administrators** dialog.
3. Select a user.
4. Click **Edit**.
5. Edit the user's email address.
6. Click **OK**.

To delete an administrative user

1. In the Launchpad, select **Administrative tasks > System configuration > Manage administrators**.
2. Click **Run**.

   This opens the **Manage Starling CertAccess administrators** dialog.

3. Select a user.
4. Click **Delete**.
5. Click **OK**.

Related topics

- Working with the Starling CertAccess Agent on page 31

Installing the Starling CertAccess Service

> IMPORTANT: Before you begin the installation, ensure that the server fulfills all the system requirements. For more information, see Starling CertAccess Agent system requirements on page 21.

The Starling CertAccess Service carries out synchronization between Starling CertAccess and the connected Active Roles environment. To install the Starling CertAccess Service, run the Server Installer program from the Launchpad. The program installs, configures, and starts the Starling CertAccess Service on a server.

> NOTE: The program performs a remote installation of the Starling CertAccess Service. Local installation of the service is not possible with this program.

> NOTE: In addition to installing the Starling CertAccess Service from the Launchpad, One Identity provides a Docker image for simple and standardized installation and running of the Starling CertAccess Service in Docker containers. You can find the Docker image and its description under https://hub.docker.com/r/oneidentity/oneim-job.

To install and configure the Starling CertAccess Service

1. In the Launchpad, select **Administrative tasks > System configuration > Install service**.
2. Click **Run**.
3. On the Server Installer start page, click **Next**.
4. When prompted, enter the configuration data for your Starling CertAccess instance.
    a. In the **Starling CertAccess configuration data** dialog, copy your Starling CertAccess Agent key into the text field.
    b. Click **OK**.
5. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
6. On the **Service access** page, enter the service's installation data.

- **Computer**: Enter the name or IP address of the server that the service is installed and started on.
- **Service account**: Enter the details of the user account that the Starling CertAccess Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the Starling CertAccess Service details, such as the installation directory, name, display name, and the Starling CertAccess Service description, using the advanced options.

7. Click **Next** to start installing the service.

   Installation of the service occurs automatically and may take some time.

8. Click **Finish** on the last page of the Server Installer.

   > NOTE: In a default installation, the service is entered in the server’s service management with the name **Starling CertAccess Service**.

Related topics

- Minimum system requirements for the Job server on page 22
- Permissions required for synchronizing with One Identity Active Roles on page 25
- Working with the Starling CertAccess Agent on page 31
- Loading the Starling CertAccess instance configuration file on page 32
- Start the Starling CertAccess Service as a Docker container on page 48
- Uninstalling the Starling CertAccess Agent on page 29

Configuring email distribution

For example, email notifications are sent if an approval decision about a request has been made or due to recertification. To use email notifications, configure how to send emails using the Launchpad. The following options are available:

- Configure distribution of email notifications through an internal SMTP server
- Secure email distribution through encryption and email signatures
- Enable approval by mail

> NOTE: Enter at least the mandatory data, otherwise email notifications cannot be sent.

To configure distribution of email notifications

1. In the Launchpad, select **Administrative tasks > System configuration > Configure email connection**.
2. Click **Run**.

3. On the home page of the Mail Configuration Wizard, click **Next**.
4. On the **Create connection to the SMTP server** page, configure the SMTP server connection to use for sending emails.
    - To test the user account data, click **Test connection**.

    - **SMTP Server**: SMTP server for sending email notifications. If a server is not given, **localhost** is used.
    - **User name**: User account name for authentication on an SMTP server.
    - **Domain**: User account domain for authentication on the SMTP server.
    - **Password** and **Password repeat**: User account password for authentication on the SMTP server.
    - **Port**: Port of the SMTP service on the SMTP server. Default: **25**
    - **Transport encryption**: Encryption method for sending email notifications. If none of the following options are given, the port is used to define the behavior (port 25: no encryption, port 465: with SSL/TLS encryption).

      Permitted values are:

        - **Auto**: Identifies the encryption method automatically.
        - **SSL**: Encrypts the entire session with SSL/TLS.
        - **STARTTLS**: Uses the STARTTLS mail server extension. Switches TLS encryption after the greeting and loading the server capabilities. The connection fails if the server does not support the STARTTLS extension.
        - **STARTTLSWhenAvailable**: Uses the STARTTLS mail server extension if available. Switches on TLS encryption after the greeting and loading the server capabilities, however, only if it supports the STARTTLS extension.
        - **None**: No security for the transport layer. All data is sent as plain text.
    - **Accept self-signed certificates**: Specifies whether self-signed certificates for TLS connections are accepted.
    - **Allow server name mismatch in certificates**: Specifies whether server names that do not match are permitted by certificates for TLS connections.
5. On the **Email settings** page, you can define the default email address of a sender and a recipient as well as the layout of the email.

    - **Recipient address**: Default email address of the recipient of the notifications.
    - **Sender address**: Sender's default email address for sending automatically generated notifications.

      Syntax:

      ```
      sender@example.com
      ```

      Example:

      ```
      NoReply@company.com
      ```

You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (**<>**).

Example:

```
One Identity <NoReply@company.com>
```

- **Language**: Default language used to send email notifications if a language cannot be determined for a recipient.
- **Language**: Default language for sending email notifications.
- **Font**: Default font for email notifications.
- **Font size**: Default font size for email notifications.
- **Signature**: Signature under the salutation.
- **Company**: Company name.
- **Link**: Link to the company's website.
- **Link display**: Display text for the link to the company's website.

6. On the **Data security** page, you can configure the data security settings.

   - **Certificate thumbprint**: SHA1 thumbprint of the certificate to use for the signature. This can be in the computer's or the user's certificate store. If you want to use a digital signature, enable **Certificate thumbprint** and enter your thumbprint.
   - **Email encryption**: Specifies whether emails are encrypted. If you enable this feature, additional settings are shown.
   - **Domain controller**: Domain controller of the requested domain to use.
   - **Domain**: Distinguished name of the domain to request.
   - **User account**:User account for querying Active Directory.
   - **Password** and **Password repeat**: Password of the user account.

7. On the **Email notifications about requests** page, make any changes to the general settings for email notifications about requests. In addition, define whether the **Approval by mail** feature can be used for requests. If you enable this feature, the settings you need are shown.

   - **Sender address**: Sender's default email address for sending automatically generated notifications.

     Syntax:

     ```
     sender@example.com
     ```

     Example:

     ```
     NoReply@company.com
     ```

     You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (**<>**).

     Example:

```
One Identity <NoReply@company.com>
```

- **Daily notifications about pending approvals**: Specifies whether approvers only receive emails once a day if there are requests awaiting their approval decisions.

  If this option is not set, approvers immediately receive an email once a request is available for approval. Set this option to reduce the number of email notifications. This will mean that you cannot use the **Approval by mail** feature.
- **IT Shop approval by mail**: Specifies whether the **Approval by mail** feature can also be used for approving requests. If you enable the feature, adjust the required settings. Then you cannot use the **Daily notifications about pending approvals** feature.
- **User name**: Name of the user account for authenticating the mailbox used for approval by mail.
- **Domain**: Domain of the user account for authenticating the mailbox used for approval by mail.
- **Password** and **Password repeat**: Password of the user account for authenticating the mailbox used for approval by mail.
- **Web service URL**: Specifies whether the URL of the Microsoft Exchange web service for accessing the mailbox is used. If you enable this functionality, enter the URL.
- **Mailbox**: Microsoft Exchange mailbox to which approvals by mail are sent.
- **Delete behavior**: Specifies the way emails are deleted from the inbox.
- **Application ID**: Exchange Online application ID for authentication with OAuth 2.0. If the value is not set, the **Basic** or the **NTML** authentication method is used.

8. On the **Email notifications about attestation** page, make any changes to the general settings for email notifications about attestations.

   Attestors are notified once a day by email if they have pending attestation cases to approve.

   - **Sender address**: Sender's default email address for sending automatically generated notifications.

     Syntax:

     ```
     sender@example.com
     ```

     Example:

     ```
     NoReply@company.com
     ```

     You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (**<>**).

     Example:

     ```
     One Identity <NoReply@company.com>
     ```

9. On the **Report subscriptions** page, you can change the default settings for report subscriptions.

    - **Sender address**: Sender's default email address for sending automatically generated notifications about report subscriptions. Replace the default address with a valid email address.

      Syntax:

      `sender@example.com`

      Example:

      `NoReply@company.com`

      You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (**<>**).

      Example:

      `One Identity <NoReply@company.com>`

    - **Default report template**: Default report that is used as a template for creating simple list reports.
    - **Store subscription**: Specifies whether subscribed reports are saved in a repository. If you enable the feature, adjust the required settings.
    - **Report storage share**: Path to the repository for subscribed reports. Syntax: `\\<Server>\<Share>`
    - **Storage life time (days)** Maximum retention period (in days) that a report is available in the storage share. After this period, reports are deleted.

10. On the **Email notifications about actions in the target system** page, you can enter an email address for notifying about actions in the target system. This might be error or success messages about changes in the target system.

    - To obtain email notifications with error or success messages about changes in the target system, enable **Active Directory** and enter the email address to send notifications to.

11. On the last page of the Mail Configuration Wizard, click **Finish**.

Related topics

- Working with the Starling CertAccess Agent on page 31

Configuring automatic assignment of identities

When you add a user account, an existing identity can automatically be assigned to it. If necessary, a new identity can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can follow on after a new user account has been created manually or through synchronization.

Identities should not automatically be assigned to administrative user accounts. Use the excluded list to specify the user accounts that do not automatically have identities assigned to them. Each entry in the list is handled as part of a regular expression.

To edit the excluded list

1. In the Launchpad, select **Administrative tasks > System configuration > Configure automatic identity assignment**.
2. Click **Run**.

   This opens the **Exclude list for automatic employee assignment** dialog.
3. To add a new entry, click **Add**.

   To edit an entry, select it and click **Edit**.
4. Enter the name of the user account that does not allow identities to be assigned automatically.

   You are allowed to use the usual special characters for regular expressions.
5. To delete an entry, select it and click **Delete**.
6. Click **OK**.

Related topics

- Working with the Starling CertAccess Agent on page 31

Configuring automatic IT Shop assignment

Synchronization ensures that Active Directory groups are automatically added to the IT Shop as products and, therefore, can be requested in the Starling CertAccess Web Portal. Certain groups may be excluded from this. Use the exclusion list to specify the groups that should not be added automatically to the IT Shop. Each entry in the list is handled as part of a regular expression.

To edit the exclude list

1. In the Launchpad, select **Administrative tasks > System configuration > Configure automatic IT Shop assignment**.
2. Click **Run**.

   This opens the **Exclude list for Active Directory groups** dialog.
3. To add a new entry, click **Add**.

   To edit an entry, select it and click **Edit**.

4. Enter the name of the group that you do not want to automatically add to the IT Shop.

   You are allowed to use the usual special characters for regular expressions.

5. To delete an entry, select it and click **Delete**.
6. Click **OK**.

Related topics

- Working with the Starling CertAccess Agent on page 31

Installing the Active Roles ADSI provider

The Starling CertAccess Agent uses the Active Roles ADSI interface for communicating with an Active Roles instance.

To establish the connection, you must install the Active Roles ADSI provider on the administrative workstation in the same version of Active Roles as the one you are going to connect. Starling CertAccess Agent supports synchronization with Active Roles versions 7.4.1, 7.4.3 and 7.4.4.

To install the Active Roles ADSI provider

1. In the Launchpad, select **Administrative tasks > Data synchronization > Install Active Roles ADSI Provider**.
2. Click **Install**.
3. Use the file explorer to select the path to the `ActiveRoles.exe` file. Select the file and click **Open**.

   This runs the installation.

   Once installing is complete, the **Install** button is grayed out in the Launchpad.

Related topics

- Starting the Starling CertAccess Launchpad on page 32

Setting up synchronization with an Active Directory domain

To manage Active Directory user accounts and groups with Starling CertAccess, set up synchronization between Active Roles and Starling CertAccess. To do this, have the following information ready:

Table 5: Information required to set up synchronization

Data	Explanation
Distinguished name of the domain.	Distinguished LDAP name of the Active Directory domain.
User account and password for logging in to Active Roles.	User account and password for logging in to Active Roles. Make a user account available with sufficient permissions. For more information, see Permissions required for synchronizing with One Identity Active Roles on page 25.
DNS name or IP address of the Active Roles server.	DNS name or IP address of the Active Roles server that connects against the synchronization server. Example: `<Name of servers>.<Fully qualified domain name>`

> IMPORTANT: Set up synchronization for all Active Directory domain that are managed by your Active Roles. Run the steps described here for each of your domains.

To set up synchronization of an Active Directory domain through Active Roles

1. In the Launchpad, select **Administrative tasks > Data synchronization > Configure Active Roles synchronization**.
2. Click **Run**.

   This starts the system connection wizard.
3. When prompted, enter the configuration data for your Starling CertAccess instance.
   a. In the **Starling CertAccess configuration data** dialog, copy your Starling CertAccess Agent key into the text field.
   b. Click **OK**.
4. On the start page of the system connection wizard, click **Next**.
5. On the **Target server** page, enter the Active Roles server to which you want to connect. If possible, servers are determined automatically.
   - In the **Host name/IP address** menu, select a target server.
   - If the server cannot be found automatically, in the **Host name/IP address** field, enter the DNS name or the IP address.
6. On the **Credentials** page, enter the user account and password for accessing Active Roles.
7. On the **Domain/root entry selection** page, select the domain you want to synchronize or enter the root entry's distinguished name.

8. On the last page of the system connection wizard, click **Finished**.

   Synchronization is now set up.

   The Launchpad shows the **Manage synchronization** task.

TIP: You can set up other Active Directory domains in the same way.

Related topics

- Working with the Starling CertAccess Agent on page 31
- Synchronization maintenance on page 44
- Loading the Starling CertAccess instance configuration file on page 32
- Minimum system requirements for administrative workstations on page 21

Synchronization maintenance

If synchronization is set up for an Active Directory domain, you can carry out the following tasks:

- Start synchronization manually
- Edit the system connection
- Delete the synchronization configuration

Related topics

- Working with the Starling CertAccess Agent on page 31
- Setting up synchronization with an Active Directory domain on page 42

Starting synchronization manually

By default, an Active Directory domain is automatically synchronized once a day. If necessary, you can start synchronization manually.

To synchronize an Active Directory domain manually

1. In the Launchpad, select **Administrative tasks > Data synchronization > Manage synchronizations**.
2. Click **Run**.
3. In the **Maintain synchronizations** dialog, select the domain.
4. Click **Start synchronization**.
5. Confirm the security prompt with **Yes**.

6. Close the alert with **OK**.

   The **Manage synchronization** dialog displays the current status of the synchronization.

Related topics

- Synchronization maintenance on page 44
- Displaying the Starling CertAccess Service log file on page 46

Editing the system connection

You can edit the system connection settings for synchronizing Active Directory domains after they have been set up. In the process, the system connection wizard is restarted.

To edit an Active Directory domain's system connection

1. In the Launchpad, select **Administrative tasks > Data synchronization > Maintain synchronizations**.
2. Click **Run**.
3. In the **Maintain synchronizations** dialog, select the domain.
4. Click **Edit system connection**.
5. Follow the system connection wizard instructions and change the relevant properties.

Related topics

- Synchronization maintenance on page 44
- Setting up synchronization with an Active Directory domain on page 42

Handling unexpected interruption of synchronization

As long as synchronization is running, certain Starling CertAccess processes are suspended. It is not possible to start synchronization again. After successful synchronization, the processes are automatically released.

If synchronization is interrupted unexpectedly, for example a server was not available, you must manually release the synchronization processes. You can only restart synchronization after this.

> IMPORTANT: Synchronization may not be reset if the regular synchronization is running.
>
> Before you reset the synchronization, ensure it has really stopped synchronizing.

To reset an interrupted synchronization

1. In the Launchpad, select **Administrative tasks > Data synchronization > Manage synchronizations**.
2. Click **Run**.
3. In the **Manage synchronizations** dialog, select the domain.
4. Click **Reset canceled synchronization**.
5. Confirm the security prompt with **Yes**.

Related topics

- Synchronization maintenance on page 44
- Displaying the Starling CertAccess Service log file on page 46

Deleting system connections

If you do not want anymore data being exchanged between an Active Directory domain and Starling CertAccess, you can delete the respective system connection. From then on, no more data will be synchronized between this domain and Starling CertAccess. Existing data that has been synchronized over this system connection up until now, remains in both systems. For more information about deleting data from a domain, see the *One Identity Starling CertAccess Web Portal User Guide*.

To delete an Active Directory domain's connection data

1. In the Launchpad, select **Administrative tasks > Data synchronization > Maintain synchronizations**.
2. Click **Run**.
3. In the **Maintain synchronizations** dialog, select the domain.
4. Click **Delete system connection**.
5. Confirm the security prompt with **Yes**.

Related topics

- Synchronization maintenance on page 44

Displaying the Starling CertAccess Service log file

You can check the current processing status in the Starling CertAccess Service log file. Use a browser front-end to show the log file. It is called up over the default port 1880.

To display the Starling CertAccess Service log file

1. In the Launchpad, select **Administrative tasks > Data synchronization > Show the service's log file**.
2. Click **Show**.

   This shows the various services of the Starling CertAccess Service in the browser.
3. To display the contents of the log file, select **Log File** in the navigation view.

The messages to be displayed on the web page can be filtered interactively. There is a menu on the website for this.

The log output is color-coded to make it easier to identify.

Table 6: Log file color code

Color	Meaning
Green	Processing successful
Yellow	Warnings occurred during processing
Red	Fatal errors occurred during processing

Related topics

- Working with the Starling CertAccess Agent on page 31
- Setting up permissions for creating an HTTP server on page 23
- Configuring how the Starling CertAccess Service log file is displayed over HTTPS on page 47

Configuring how the Starling CertAccess Service log file is displayed over HTTPS

In order for the Starling CertAccess Service's log file to be accessible over HTTPS, additional configuration settings are required.

1. Configure the certificate in the operating system.

   The Starling CertAccess Service uses `System.Net.HttpListener` for the web interface. `System.Net.HttpListener` can be configured to use a certificate for specific ports using `HttpCfg.exe`. For detailed information on how to configure certificates, see How to: Configure a port with an SSL certificate.
2. Customize the Starling CertAccess Service configuration. Enable the **Use SSL** parameter (`UseSSL`) in the configuration file of the Starling CertAccess Service. Use the Job Service Configuration program to do this.

To configure how to display the Starling CertAccess Service log file over HTTPS

a. Run the `JobServiceConfigurator.exe` file from the Starling CertAccess Service's install directory.

   This loads the Starling CertAccess Service's configuration file (`Jobservice.cfg`) from the install directory. The path of the loaded file is displayed in the Job Service Configuration's title bar.

b. In Job Service Configuration, select the **Configuration** entry and enable the **Use SSL** option.

c. To save the change, select **File > Save**.

The change will be applied while the Starling CertAccess Service is running. The Starling CertAccess Service does not need to be restarted.

Start the Starling CertAccess Service as a Docker container

The Starling CertAccess Service carries out synchronization between Starling CertAccess and the connected Active Roles environment. In addition to installing the Starling CertAccess Service from the Launchpad, One Identity provides a Docker image for simple and standardized installation and running of the Starling CertAccess Service in Docker containers. For the Starling CertAccess Service connection to Active Roles, you must build this Docker image on your Windows Docker host because the Active Roles ADSI Provider must be installed in the version matching the Active Roles version. Use the One Identity Manager Docker image that is supplied in the Docker hub as basis.

To create a Docker image for your Starling CertAccess Service

1. Create a new directory on your Windows Docker host.
2. In this directory, create a `files` subdirectory.
3. Copy the `ActiveRoles.exe` installation file that matches your version of the Active Roles server into this subdirectory.
4. In the main directory, create a file with the name `Dockerfile` and the following content:

```
# base image (see https://hub.docker.com/r/oneidentity/oneim-job)
FROM oneidentity/oneim-job:windows-amd64-latest-windowsservercore-1903

# copy and install Active Roles ADSI Provider
COPY files/ActiveRoles.exe /Installer/
RUN C:/installer/ActiveRoles.exe /quiet /install ADDLOCAL=Tools
/IAcceptActiveRolesLicenseTerms
```

5. To build the Docker image, open a command line console in the main directory and run the following command:

   ```
   docker build -t local/oneim-job-ars:windows-amd64-latest-
   windowsservercore-1903 .
   ```

   Once the build process is complete, the Docker image is available with the name l**ocal/oneim-job-ars:windows-amd64-latest-windowsservercore-1903.**

To start the Docker container

1. Define the following parameters as secret or as environment variables.

   HTTP_User

   User name required for accessing the service's status website.

   HTTP_PWD

   Password required for accessing the service's status website.

   CLOUDCONFIG

   Connection string of your Starling CertAccess instance that is made available for your instance on the Starling CertAccess website.

2. Start the container.

Example of starting the container through Windows PowerShell

In this example, the parameters are set as secrets.

```
$secrets='C:\Path\To\secrets'

# Create directory
New-Item -ItemType Directory -Force -Path "$secrets"

# Create secrets
Set-Content -NoNewline -Path "$secrets\HTTP_USER" -Value "<user for status
website>"
Set-Content -NoNewline -Path "$secrets\HTTP_PWD" -Value "<password for status
website>"
Set-Content -NoNewline -Path "$secrets\CLOUDCONFIG" -Value "<connetion string>"

# Create Container
docker run -d `
--name "StarlingCertAccessService" `
--hostname "DockerService" `
--cpus="4.0" `
-m 4GB `
-p 1880:1880 `
-v $secrets/:C:/ProgramData/Docker/secrets:ro `
local/oneim-job-ars:windows-amd64-latest-windowsservercore-1903
```

For more information about One Identity Manager Docker images, see https://hub.docker.com/r/oneidentity/oneim-job.

Related topics

- Installing the Starling CertAccess Service on page 35

Appendix A

Mapping Active Roles schema types in Starling CertAccess

To manage Active Directory user accounts and groups with Starling CertAccess, set up synchronization between Active Roles and Starling CertAccess. The schema types are mapped to each other as follows.

Table 7: Schema type mapping

Schema type in Active Roles	Schema type in Starling CertAccess
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
msExchSystemObjectsContainer	ADSContainer
oganization	ADSContainer
organizationalUnit	ADSContainer
printQueue	ADSPrinter
rpcContainer	ADSContainer
user	ADSAccount

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

Index