One Identity Starling Governance

Administration Guide for One Identity Active Roles Integration

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 Governance Administration Guide for One Identity Active Roles Integration
Updated - 12 May 2021, 03:13

Contents

1

About this guide

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

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

The *One Identity Starling Governance Administration Guide for One Identity Active Roles Integration* is aimed at Active Roles administrators that utilize Starling Governance 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 Governance Web Portal User Guide*.

Available documentation

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

2

Starling Governance basics

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

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

Users can use Starling Governance 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 Governance 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.

Starling Governance is integrated as a service in One Identity Starling (https://cloud.oneidentity.com). You can subscribe to a trial version of the 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 Governance if it is supported by One Identity Starling. For more information about this, see the *One Identity Starling User Guide*.

Additional hardware and software prerequisites

The hardware and software prerequisites for One Identity Starling apply to Starling Governance. 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 Governance as a service

To use Starling Governance as a Starling service, you require a Starling organization. You can add the Starling Governance 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 the Starling Governance service to it. You can select the following subscription types for Starling Governance:

- Paid subscriptions on page 9
- Trial subscriptions on page 7

Trial subscriptions

Starling Governance 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 Governance will no longer be accessible.

You can trial Starling Governance in two ways.

1. If you want to see how the main functions of Starling Governance 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 Governance 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 Governance with your own One Identity Active Roles installation, then you can request a Proof of Concept trial. This will allow you to trial Starling Governance Web Portal functions and also let you see how data is synchronized between your own Active Roles and Starling Governance. 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 9
- Using Starling Governance as a service on page 7

Starting a trial subscription

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

To start a trial subscription

1. Sign in to Starling.
2. On the home page, select Starling Governance Service 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 Governance to your organization.
4. Click **Confirm**.
5. Enter a domain name for your Starling Governance 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 Governance Agent and set up synchronization with your One Identity Active Roles.

   For more information, see Setting up initial synchronization on page 12.

9. If you have started a Demo trial, on the Starling Governance website, click **Go**.

   This opens the Starling Governance Web Portal.

Then the Governance Service 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 Governance tile to find out how you can purchase the product.

Related topics

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

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 Governance website, click the **End Trial** button.
2. Click **OK**.

Related topics

- Starting a trial subscription on page 8
- Paid subscriptions on page 9

Paid subscriptions

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

   Once the subscription has been set up and your Starling Governance 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 Governance 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 Governance 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 Governance Agent and set up your One Identity Active Roles synchronization.

   For more information, see Setting up initial synchronization on page 12.

Related topics

- Paid subscriptions on page 9

Updating the Starling Governance instance

From time to time, your Starling Governance 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 Governance website. If the instance is not accessible, all users see an appropriate message.

Setting up initial synchronization

After you have prepared the Starling Governance service for your organization, you can then set up the initial synchronization with Active Roles. To do this, install the Starling Governance Agent on an administrative workstation. Ensure that all the system requirements are fulfilled. For more information, see Starling Governance Agent system requirements on page 19.

To set up synchronization with Active Roles

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

   This opens the Starling Governance website.
2. Download the Starling Governance Agent installation package onto a workstation.
   a. Under **Step 1**, click **Download Agent**.
   b. Copy the Starling Governance Agent key into the clipboard. Under **Step 2**, click **Copy**.

      IMPORTANT: Save your Starling Governance Agent key in a safe place because you will need it later.
3. Install the Starling Governance Agent on the workstation.

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

      This starts the installation wizard.
   c. On the start page, select the language for the installation wizard.
   d. Confirm the conditions of the license.
   e. 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 Governance 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 last page of the installation wizard, click **Start** to run the Starling Governance Agent Launchpad.

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

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

ii. Click **OK**.

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

4. The first time you start the Launchpad, the Starling Governance Agent is updated automatically. This loads the newest version of the Starling Governance Agent and installs it.

- Click **Yes**.

5. Sign in with your Starling credentials.

- Click **Next**.

This starts the Launchpad.

6. Install the Starling Governance Agent Service.

The Starling Governance Agent Service is installed remotely on a Job server.

Prerequisites:

a. The server fulfills the minimum system requirements. For more information, see Minimum system requirements for the Job server on page 20.

b. A user account is available in your Active Roles with the following permissions:

- All Objects - Read All Properties
- All Objects - Full Control
- Member in the Active Roles administrators group

This user account is entered as the service account for the Starling Governance Agent Service.

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**: Name or IP address of the server that the service is installed and started on.
- **Service account**: User account data for the Starling Governance Agent Service.
  - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation. Use the user account that you provided in your Active Roles for this purpose.
- **Installation account**: Data for the administrative user account to install the service.
  - To use the current user's account, set the **Use current user** option.
  - To use another user account, disable the **Use current user** option and enter the user account, password and password confirmation.
- To change the install directory, names, display names or description of the Starling Governance Agent Service, use the additional settings.

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 Governance Agent 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 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.

Use the user account that you entered as the service account for the Starling Governance Agent Service.

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 > Maintain 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**.

TIP: You can display the Starling Governance Agent Service log in a browser. The log file shows you the synchronization's progress. Here you can check that the Starling Governance Agent Service is working correctly.

For more information, see Displaying the Starling Governance Agent Service log file on page 41.

If synchronization is complete, you will see the synchronized data in the Governance Portal.

10. Check that the data has been synchronized correctly.

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

This opens the Governance 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 Governance Web Portal, see *One Identity Starling Governance Web Portal User Guide*.

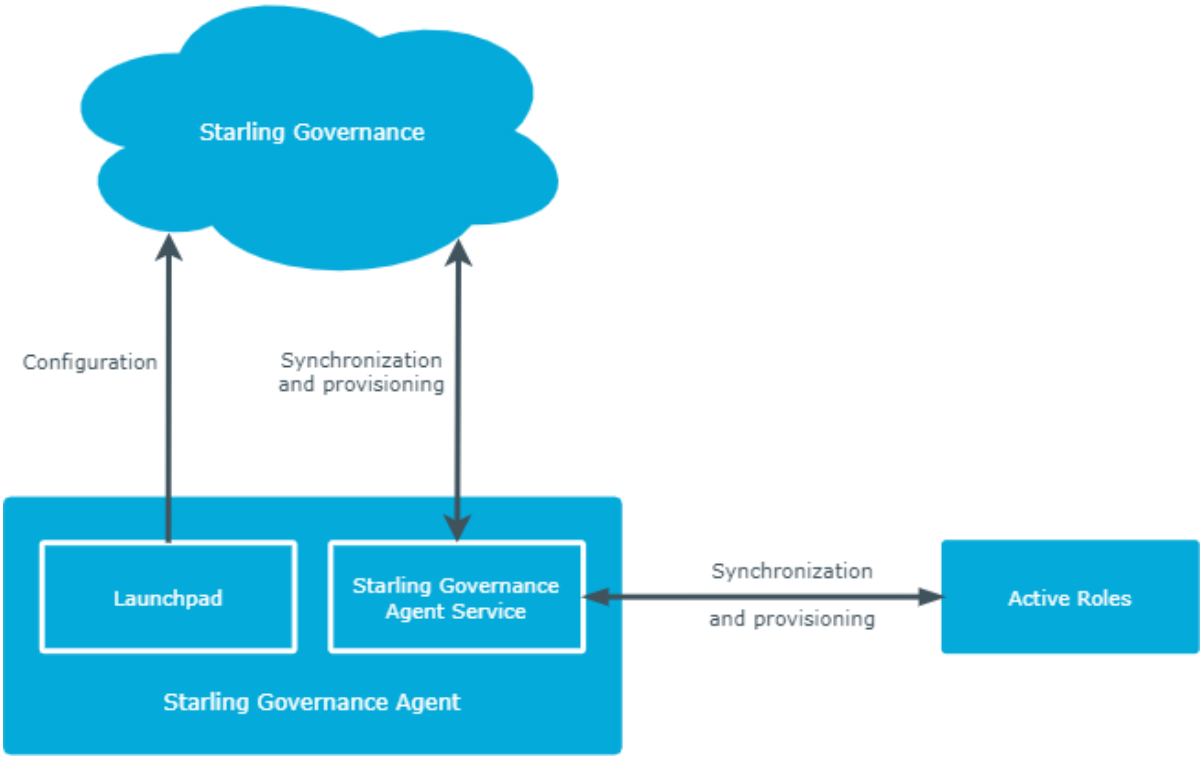
Detailed information about this topic

- Installing the Starling Governance Agent on a workstation on page 25
- Installing the Starling Governance Agent Service on page 31
- Minimum system requirements for the Job server on page 20
- Starling Governance Agent Service permissions required for synchronizing with One Identity Active Roles on page 24
- Installing the Active Roles ADSI provider on page 37
- Setting up synchronization with an Active Directory domain on page 38

Starling Governance Agent architecture

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

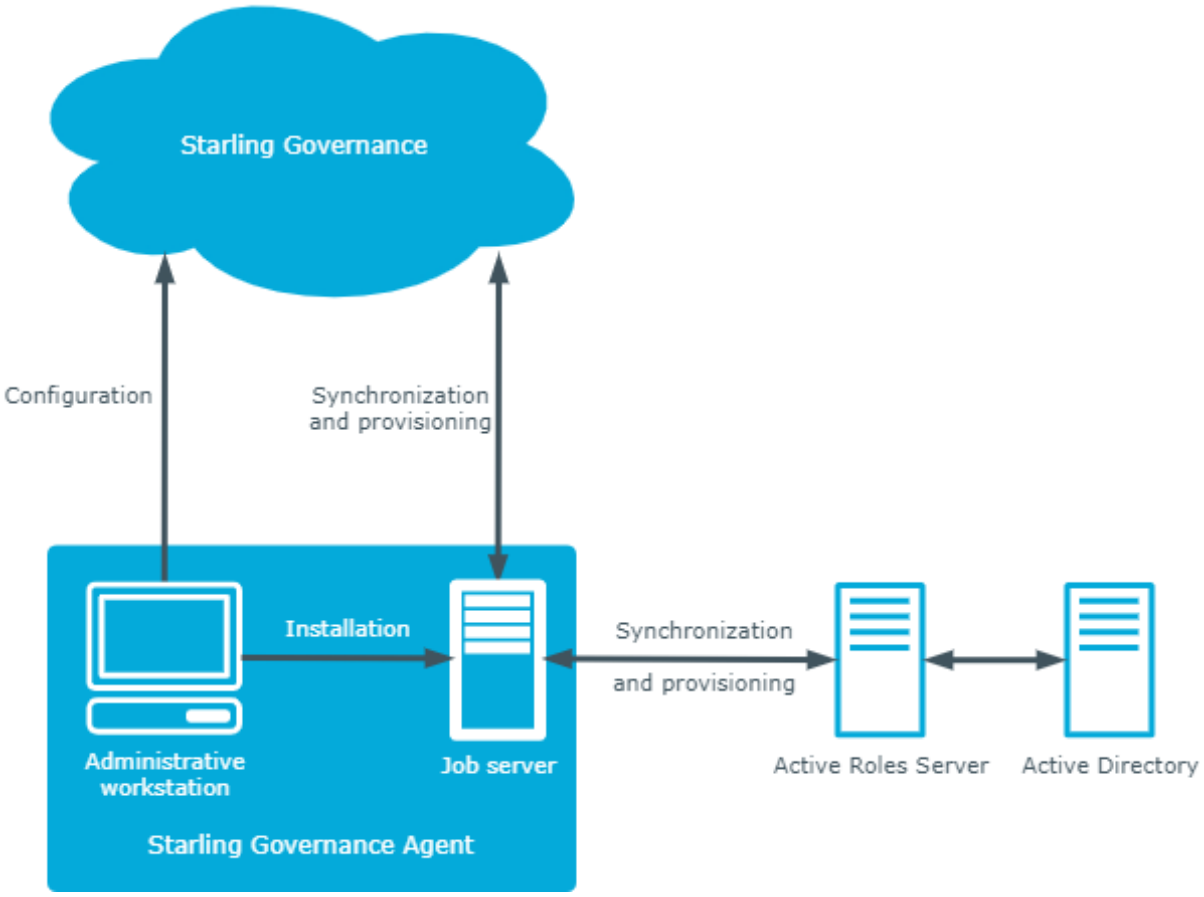
Figure 1: Starling Governance Agent architecture



You install the Starling Governance Agent on an administrative workstation. Then you can start the Starling Governance Agent Launchpad and use it to install the Starling Governance Agent Service on a Job server. The Starling Governance Agent Service carries out

synchronization of the Active Directory environment that is connected through One Identity Active Roles.

Figure 2: Starling Governance Agent topology



Starling Governance Agent system requirements

The following installation prerequisites represent the minimum requirements for installing and unlimited operation of the Starling Governance Agent.

Every Starling Governance Agent installation can be virtualized. Ensure that performance and resources are available to the respective Starling Governance Agent component according to system requirements. Virtualization of a Starling Governance 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 Governance 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 • 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	• Internet Explorer 11 or later • Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (release channel)

Minimum system requirements for the Job server

The Starling Governance Agent Service enables the distribution throughout the network of data that is administrated in Starling Governance. The Starling Governance Agent Service carries out the following tasks:

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

The following system prerequisites must be fulfilled to install the Starling Governance Agent 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 Governance Agent Service, you must have an administrative workstation on which the Starling Governance Agent components are installed.

Related topics

- Installing the Starling Governance Agent Service on page 31
- Minimum system requirements for administrative workstations on page 19

Setting up permissions for creating an HTTP server

The log files of the Starling Governance Agent 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 Governance Agent 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 Governance Agent is made up of several components that can run in different network segments. In addition, Starling Governance 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 Governance.
1880	Port for the HTTP protocol of Starling Governance Agent Service.

Default port	Description
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 Governance Agent users

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

Table 4: Starling Governance Agent users

User	Authorizations
User for logging into the Starling Governance Agent	By default, the user that you used to initially register for One Identity Starling has administrative permissions for the Starling Governance Agent. This user can grant other administrative users access to the Starling Governance Agent. Users that login to the Starling Governance Agent Launchpad are authenticated with OAuth 2.0.
User account for the Starling Governance Agent Service	The user account for the Starling Governance Agent 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 Governance Agent 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 Governance Agent Service installation directory in order to automatically update Starling Governance Agent. In the default installation, Starling Governance Agent is installed

User	Authorizations
	under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)

Related topics

- Managing Starling Governance Agent administrators on page 30
- Starling Governance Agent Service permissions required for synchronizing with One Identity Active Roles on page 24

Starling Governance Agent Service permissions required for synchronizing with One Identity Active Roles

It is recommended that you set up a special user account for Active Directory, which is used for connecting to Active Roles through the Starling Governance Agent Service. 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 One Identity Active Roles Access Templates, see your *Active Roles documentation*.

The following Access Templates are suggested for delegating permissions:

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

Starling Governance Agent works without controlling Active Roles workflows. To avoid existing Active Roles workflows, you must add the user account to the Active Roles administrators group. This group is created during Active Roles installation. The name of the group is saved in the registry database under:

- Registration key: HKEY_Local_Machine\Software\Aelita\Enterprise Directory Manager
- Value: DSAdministrators

Installing the Starling Governance Agent on a workstation

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

IMPORTANT: Before you begin the installation, ensure that the workstation fulfills all the system requirements. For more information, see Starling Governance Agent system requirements on page 19.

To install the Starling Governance Agent

1. Unpack the Starling Governance 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 Governance 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 last page of the installation wizard, click **Start** to run the Starling Governance Agent Launchpad.
7. Click **Finish** to close the installation wizard.

Starling Governance Agent is installed for all user accounts on the workstation. In the default installation, Starling Governance 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 Governance Agent on page 27
- Starting the Starling Governance Agent Launchpad on page 28

Working with the Starling Governance Agent

Use the Starling Governance Agent to set up synchronization between an Active Roles managed Active Directory environment and Starling Governance. 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 Governance. Changes to Active Directory group memberships in Starling Governance are published immediately in the Active Directory domain.

Use the Starling Governance Agent to perform the following:

- Manage Starling Governance Agent administrators
- Install the Starling Governance Agent 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 Governance Agent Service's status
- Configure automatic approval

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

Detailed information about this topic

Starting the Starling Governance Agent Launchpad

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

To start the Launchpad

1. In the Windows start menu, select **Starling Governance Agent Launchpad**.
2. When prompted, enter the configuration data for your Starling Governance instance.
    a. In the **Starling Governance configuration data** dialog, copy your Starling Governance Agent key into the text field.
    b. Click **OK**.
3. Sign in with your Starling credentials.
4. Click **Next**.

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

Related topics

- Working with the Starling Governance Agent on page 27
- Loading the Starling Governance instance configuration file on page 28

Loading the Starling Governance instance configuration file

To communicate with Starling Governance, the Starling Governance Agent requires the Starling Governance Agent key of your Starling Governance 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 Governance Agent key

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

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

To load the configuration data

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

Related topics

- Setting up initial synchronization on page 12
- Working with the Starling Governance Agent on page 27
- Starting the Starling Governance Agent Launchpad on page 28
- Installing the Starling Governance Agent Service on page 31
- Setting up synchronization with an Active Directory domain on page 38

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 Governance 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 Governance Agent Launchpad on page 28

Managing Starling Governance Agent administrators

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

Starling Governance Agent administrators are automatically granted administrative permissions for Starling Governance. They are target system managers for Active Roles, they manage identities, configure attestations and the IT Shop for requests.

To add an administrative user

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

   This opens the **Maintain Starling Governance Agent 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 > Maintain administrators**.
2. Click **Run**.

   This opens the **Maintain Starling Governance Agent 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 > Maintain administrators**.
2. Click **Run**.

   This opens the **Maintain Starling Governance Agent administrators** dialog.
3. Select a user.
4. Click **Delete**.
5. Click **OK**.

Related topics

- Working with the Starling Governance Agent on page 27

Installing the Starling Governance Agent Service

IMPORTANT: Before you begin the installation, ensure that the server fulfills all the system requirements. For more information, see Starling Governance Agent system requirements on page 19.

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

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

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

To install and configure the Starling Governance Agent 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 Governance instance.
    a. In the **Starling Governance configuration data** dialog, copy your Starling Governance 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**: Name or IP address of the server that the service is installed and started on.
    - **Service account**: User account data for the Starling Governance Agent Service.

- To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation. Use the user account that you provided in your Active Roles for this purpose.

- **Installation account**: Data for the administrative user account to install the service.
  - To use the current user's account, set the **Use current user** option.
  - To use another user account, disable the **Use current user** option and enter the user account, password and password confirmation.
- To change the install directory, names, display names or description of the Starling Governance Agent Service, use the additional settings.

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 Governance Agent Service**.

Related topics

- Minimum system requirements for the Job server on page 20
- Working with the Starling Governance Agent on page 27
- Loading the Starling Governance instance configuration file on page 28
- Start the Starling Governance Agent Service as a Docker container on page 42

Configuring email distribution

The Starling Governance Agent provides a configuration for sending email notifications to Starling Governance users. For example, users are notified by email if an approval decision is made about a request or on recertification. You can customize email notification settings in the Launchpad. You might want to use a mailbox in your Microsoft Exchange or Exchange Online environment. 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

To configure distribution of email notifications

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

3. On the start 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 function, 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 and define whether the **Approval by mail** function can be used for requests. If you enable the function, the necessary settings 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>
```

- **IT Shop approval by mail**: Specifies whether the **Approval by mail** function can also be used for approving requests. If you enable the function, adjust the required settings.
- **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 attestation and define whether the **Approval by mail** function can be used for attestation. If you enable the function, the necessary settings 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>
     ```

   - **Attestation by mail**: Specifies whether the function **Approval by mail** can be used. If you enable the function, adjust the required settings.
   - **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.

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 function, 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 Governance Agent on page 27

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 Governance Agent on page 27

Installing the Active Roles ADSI provider

The Active Roles Starling Governance Agent connector uses the Active Roles ADSI interface for communicating with an Active Roles instance. The Active Roles connector is used for synchronization and provisioning Active Directory. The Active Roles connector connects to an Active Roles instance, which then connects to the Active Directory domain controller.

In order to establish a connection, you must install the Active Roles ADSI provider on the administrative workstation.

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 Governance Agent Launchpad on page 28

Setting up synchronization with an Active Directory domain

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

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 into Active Roles.	User account and password for logging into Active Roles. Make a user account available with sufficient permissions. For more information, see Starling Governance Agent Service permissions required for synchronizing with One Identity Active Roles on page 24.
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 synchronization**.
2. Click **Run**.

   This starts the system connection wizard.
3. When prompted, enter the configuration data for your Starling Governance instance.

   a. In the **Starling Governance configuration data** dialog, copy your Starling Governance 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.

   Use the user account that you entered as the service account for the Starling Governance Agent Service.
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 Governance Agent on page 27
- Synchronization maintenance on page 39
- Loading the Starling Governance instance configuration file on page 28
- Minimum system requirements for administrative workstations on page 19

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 Governance Agent on page 27
- Setting up synchronization with an Active Directory domain on page 38

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 > Maintain 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**.

Related topics

- Synchronization maintenance on page 39
- Displaying the Starling Governance Agent Service log file on page 41

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 39
- Setting up synchronization with an Active Directory domain on page 38

Deleting system connections

If you do not want anymore data being exchanged between an Active Directory domain and Starling Governance, you can delete the respective system connection. From then on, no more data will be synchronized between this domain and Starling Governance. Existing data that has been synchronized over this system connection up until now, remains in both systems.

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 39

Displaying the Starling Governance Agent Service log file

You can check the current processing status in the Starling Governance Agent 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 Governance Agent 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 Governance Agent 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 Governance Agent on page 27
- Setting up permissions for creating an HTTP server on page 22

Start the Starling Governance Agent Service as a Docker container

The Starling Governance Agent Service carries out synchronization between Starling Governance and the connected Active Roles environment. In addition to installing the Starling Governance Agent Service from the Launchpad, One Identity provides a Docker image for simple and standardized installation and running of the Starling Governance Agent Service in Docker containers. For the Starling Governance Agent 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 Governance Agent 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 **local/oneim-job-ars:windows-amd64-latest-windowsservercore-1903**.

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 Governance instance that is made available for your instance on the Starling Governance 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 "StarlingGovernanceAgentService" `
--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 Governance Agent Service on page 31

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

T

U

W