ONE IDENTITY

by Quest

Connect for Safeguard Assets 7.5

User Guide

Contents

Connect for Safeguard Assets

Introduction to Connect for Safeguard Assets

Accessible from the Starling site (https://www.cloud.oneidentity.com/), Connect for Safeguard Assets is designed to extend the capabilities of Safeguard for Privileged Passwords to allow for disconnected assets to be discovered and managed by Safeguard for Privileged Passwords.

> IMPORTANT: In order to use Connect for Safeguard Assets you need a Starling organization and account within either the United States or European Union data center. For more information on Starling organizations, see the Starling documentation.

> IMPORTANT: In order to use Connect for Safeguard Assets some additional software and hardware requirements are required. For more information, see Additional hardware and software requirements.

Additional hardware and software requirements

Features available within Connect for Safeguard Assets have additional requirements beyond those necessary for Starling overall (for more information, see the *Starling User Guide*).

Connect for Safeguard Assets requirements

Table 1: Connect for Safeguard Assets requirements

Requirement	Description
Safeguard for	Safeguard for Privileged Passwords 7.1 or later joined to your

Requirement	Description
Privileged Passwords 7.1 or later	Starling organization. For more information, see Safeguard for Privileged Passwords documentation.
Available Agent versions	The versions supported for each of the available agents listed on the **Downloads** page are listed in the *Supported platforms* section of the *One Identity Safeguard for Privileged Passwords Administration Guide* (for more information, see Safeguard for Privileged Passwords documentation).

Supported platforms

Table 2: Supported platforms

Agent Name	Platform Name	Tested Versions
Linux (Connect)	CentOS Linux	CentOS Linux 7
		CentOS Linux 8
	Debian GNU/Linux	Debian GNU/Linux 9
		Debian GNU/Linux 10
		Debian GNU/Linux 11
	Fedora	Fedora 37
		Fedora 38
	Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 7
		Red Hat Enterprise Linux (RHEL) 8
	Rocky Linux	Rocky Linux 8
		Rocky Linux 9
	SUSE Linux Enterprise Desktop (SLED)	SUSE Linux Enterprise Desktop (SLED) 12
		SUSE Linux Enterprise Desktop (SLED) 15
	SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 12
		SUSE Linux Enterprise Server (SLES) 15
	Ubuntu	Ubuntu 18.04 LTS
		Ubuntu 22.04 LTS
		Ubuntu 22.10

Agent Name	Platform Name	Tested Versions
		Ubuntu 23.04
macOS (Connect)	macOS	macOS 11 Intel x86 64, ARM64
		macOS 12 Intel x86 64, ARM64
		macOS 13 Intel x86 64, ARM64
Windows Desktop (Connect)	Windows	Windows 10 x64
		Windows 11 x64
Windows Server (Connect)	Windows Server	Windows Server 2012 x64
		Windows Server 2012 R2 x64
		Windows Server 2016 x64
		Windows Server 2019 x64
		Windows Server 2022 x64

Getting started

Using the Connect for Safeguard Assets service

Once you have added the Connect for Safeguard Assets service to your Starling organization, you have full access to the Connect for Safeguard Assets service which can be used in conjunction with Safeguard for Privileged Passwords to manage assets that are not connected to a corporate network.

To navigate through the service use the title bar along the top of the site, which contains the following links:

- ▦ : If multiple organizations are associated with your account, this button (displaying the name of the organization you are currently viewing) appears and opens a drop-down menu that allows you to move between organizations.

- �◼ : This button (displaying the first name of the account owner) opens a drop-down menu that allows you to select one of the following options:
    - **My Services**: Clicking this link takes you to the Starling home page.
    - **Sign out**: Clicking this link signs you out of Starling.

- ⚙ : Clicking this link opens the settings page where you can manage your entire Starling account. For more information, see the *One Identity Starling User Guide*.

The main pages available within Connect for Safeguard Assets are listed in the navigation bar, which is located beneath the title bar:

- Downloads page: This is the home page of Connect for Safeguard Assets and provides insight into your service.

- Collaborators page: This page is used to add additional collaborators to your Connect for Safeguard Assets service.

- Agents page: This page is used to monitor the status of configured agents.

Downloads page

Upon opening Connect for Safeguard Assets, you will be directed to the **Downloads** page. This page contains a list of the platforms that Connect for Safeguard Assets supports connecting with in order to manage the associated assets. By connecting to these assets via Connect for Safeguard Assets instead of directly from Safeguard for Privileged Passwords, you are able to manage the assets without requiring they be connected to a corporate network.

Available Agents

This section contains the agent downloads for each of the supported platforms. Each agent tile displays the name of the platform it supports, the agent version, and a **Download** button.

Windows

For more information, see Downloading a Windows agent.

Mac

For more information, see Downloading a Mac agent.

Linux

For more information, see Downloading a Linux agent.

Tokens

This section contains token downloads.

Agent Enrollment

For more information, see Downloading an Agent Enrollment token.

Downloading a Windows agent

The following explains the process for downloading and installing a Windows agent on a disconnected asset. The same token and agent binaries can be used by multiple machines which (depending on your organization's environment) may allow for this to be pushed out to multiple machines rather than having to manually install an agent on each individual machine.

To download a Windows agent

1. On the **Downloads** page, click the **Download** button associated with the **Windows** tile.

    A zipped `ConnectForSafeguardWindowsAgent` folder will be downloaded according to your browser settings.

2. Unzip the `ConnectForSafeguardWindowsAgent` folder.

3. To the extracted `ConnectForSafeguardWindowsAgent` folder, add the agent enrollment token file (Downloading an Agent Enrollment token).

    > ⚠️ **CAUTION: Keep a copy of the enrollment token until the agent has been successfully enrolled. The token file will be automatically removed after each enrollment attempt (including failed attempts).**

4. Open a Command Prompt or PowerShell session.

5. Run the `enroll` command on `ConnectForSafeguardAssetsAgent.exe`. The local service account used for enrollment must be a member of the local administrators group and have the **Log on as a service** permission either explicitly or via a group.

    Once the agent has been successfully enrolled, the **Safeguard Disconnected Asset Agent** will be installed under the service account along with a **ConnectForSafeguardAssets** certificate that is valid for 60 days. The agent will automatically attempt to renew the certificate after 30 days have passed since the last certificate was issued. However, if an agent is unable to re-enroll and the certificate expires, the re-enroll command can be used to re-enroll the agent (for more information, see Re-enrolling an installed agent).

6. In Safeguard for Privileged Passwords, you can now add or discover the asset (using the **Windows Desktop (Starling Connect)** or **Windows Server (Starling Connect)** platforms). For more information, see the *One Identity Safeguard for Privileged Passwords Administration Guide*.

    Make sure the `Agent ID` is the same as shown in Safeguard for Privileged Passwords (**Assets** > (select asset) > **Properties** > **Connection** > 🖉 (Edit) > **StarlingAgentID**). If the `Agent ID` is different, you need to update the **StarlingAgentID** in Safeguard for Privileged Passwords to match the `Agent ID`.

    > NOTE: When running a password task in Safeguard for Privileged Passwords against a Windows agent, the task is created in a submitted state and will be updated once the agent processes the task. The amount of time this will take to update will vary depending upon the state of the machine the agent is running on.

Downloading a Mac agent

The following explains the process for downloading and installing a Mac agent on a disconnected asset. The same token and agent binaries can be used by multiple machines which (depending on your organization's environment) may allow for this to be pushed out to multiple machines rather than having to manually install an agent on each individual machine. There are 2 Mac agents to select from depending on your environment:

- Mac x64 agent
- Mac arm64 agent

Mac x64 agent

To download a Mac x64 agent

1. On the **Downloads** page, click the **Download** button associated with the Mac x64 tile.

   A zipped `ConnectForSafeguardMacAgent` folder will be downloaded according to your browser settings.

2. Unzip the `ConnectForSafeguardMacAgent.zip` folder.

3. To the extracted `ConnectForSafeguardMacAgent` folder, add the agent enrollment token file (Downloading an Agent Enrollment token).

   ⚠ **CAUTION: Keep a copy of the enrollment token until the agent has been successfully enrolled. The token file will be automatically removed after each enrollment attempt (including failed attempts).**

4. Right-click the `appsettings.json` file and select to run a command line prompt. The service account used for enrollment must be a member of **sudoers**.

5. From a terminal, the `enroll` command on the `ConnectForSafeguardAssetsAgent` executable.

   Once the agent has been successfully enrolled, the **Safeguard Disconnected Asset Agent** will be installed under the service account along with a **ConnectForSafeguardAssets** certificate that is valid for 60 days. The agent will automatically attempt to renew the certificate after 30 days have passed since the last certificate was issued. However, if an agent is unable to re-enroll and the certificate expires, the re-enroll command can be used to re-enroll the agent (for more information, see Re-enrolling an installed agent).

6. In Safeguard for Privileged Passwords, you can now add or discover the asset (using the **macOS (Starling Connect)** platform). For more information, see the *One Identity Safeguard for Privileged Passwords Administration Guide*.

   Make sure the `Agent ID` is the same as shown in Safeguard for Privileged Passwords (**Assets** > (select asset) > **Properties** > **Connection** > 🖉 (Edit) > **StarlingAgentID**). If the `Agent ID` is different, you need to update the **StarlingAgentID** in Safeguard for Privileged Passwords to match the `Agent ID`.

NOTE: When running a task in Safeguard for Privileged Passwords against a Mac agent, the task is created in a submitted state and will be updated once the agent processes the task. The amount of time this will take to update will vary depending upon the state of the machine the agent is running on.

Mac arm64 agent

To download a Mac arm64 agent

1. On the **Downloads** page, click the **Download** button associated with the Mac arm64 tile.

   A zipped `ConnectForSafeguardMacArm64Agent` folder will be downloaded according to your browser settings.

2. Unzip the `ConnectForSafeguardMacArm64Agent.zip` folder.

3. To the extracted `ConnectForSafeguardMacArm64Agent` folder, add the agent enrollment token file (Downloading an Agent Enrollment token).

4. Right-click the `appsettings.json` file and select to run a command line prompt. The service account used for enrollment must be a member of **sudoers**.

5. From a terminal, the `enroll` command on the `ConnectForSafeguardAssetsAgent` executable.

   Once the agent has been successfully enrolled, the **Safeguard Disconnected Asset Agent** will be installed under the service account along with a **ConnectForSafeguardAssets** certificate that is valid for 60 days. The agent will automatically attempt to renew the certificate after 30 days have passed since the last certificate was issued. However, if an agent is unable to re-enroll and the certificate expires, the re-enroll command can be used to re-enroll the agent (for more information, see Re-enrolling an installed agent).

6. In Safeguard for Privileged Passwords, you can now add or discover the asset (using the **macOS (Starling Connect)** platform). For more information, see the *One Identity Safeguard for Privileged Passwords Administration Guide*.

   Make sure the `Agent ID` is the same as shown in Safeguard for Privileged Passwords (**Assets** > (select asset) > **Properties** > **Connection** > ✐ (Edit) > **StarlingAgentID**). If the `Agent ID` is different, you need to update the **StarlingAgentID** in Safeguard for Privileged Passwords to match the `Agent ID`.

   NOTE: When running a task in Safeguard for Privileged Passwords against a Mac agent, the task is created in a submitted state and will be updated once the agent processes the task. The amount of time this will take to update will vary depending upon the state of the machine the agent is running on.

Downloading a Linux agent

The following explains the process for downloading and installing a linux agent on a disconnected asset. The same token and agent can be used by multiple machines which (depending on your organization's environment) may allow for this to be pushed out to

multiple machines rather than having to manually install an agent on each individual machine.

To download a Linux agent

IMPORTANT: If `requiretty` is enabled on your linux machine, you need to add the following line to the sudoers file:

`Defaults:<service account name> !requiretty`

1. On the **Downloads** page, click the **Download** button associated with the **Linux** tile.

   A zipped `ConnectForSafeguardLinuxAgent` folder will be downloaded according to your browser settings.

2. Unzip the `ConnectForSafeguardLinuxAgent.zip` folder.

3. To the unzipped `ConnectForSafeguardLinuxAgent.zip` folder, add the agent enrollment token file (Downloading an Agent Enrollment token).

   > ⚠️ **CAUTION: Keep a copy of the enrollment token until the agent has been successfully enrolled. The token file will be automatically removed after each enrollment attempt (including failed attempts).**

4. Change the permissions on the `ConnectForSafeguardAssetsAgent` file (chmod 750) to make it executable.

5. Using a service account that is a member of sudoers (you may need to run `sudo ConnectForSafeguardAssetsAgent`), run the `enroll` command on `ConnectForSafeguardAssetsAgent`.

   Once the agent has been successfully enrolled, the **Safeguard Disconnected Asset Agent** will be installed under the service account along with a **SafeguardAssetsAgent** certificate that is valid for 60 days. The agent will automatically attempt to renew the certificate after 30 days have passed since the last certificate was issued. However, if an agent is unable to re-enroll and the certificate expires, the re-enroll command can be used to re-enroll the agent (for more information, see Re-enrolling an installed agent).

6. In Safeguard for Privileged Passwords, you can now add or discover the asset (using the **Linux (Starling Connect)** platform). For more information, see the *One Identity Safeguard for Privileged Passwords Administration Guide*.

   Make sure the `Agent ID` is the same as shown in Safeguard for Privileged Passwords (**Assets** > (select asset) > **Properties** > **Connection** > ✎ (Edit) > **StarlingAgentID**). If the `Agent ID` is different, you need to update the **StarlingAgentID** in Safeguard for Privileged Passwords to match the `Agent ID`.

   > NOTE: When running a task in Safeguard for Privileged Passwords against a Linux agent, the task is created in a submitted state and will be updated once the agent processes the task. The amount of time this will take to update will vary depending upon the state of the machine the agent is running on.

Downloading an Agent Enrollment token

The agent enrollment token (30 day sliding expiration with a 90 day limit) needs to be added to the folder.

To download an Agent Enrollment token

1. On the **Downloads** page, click the **Download** button associated with the **Agent Enrollment** tile.

   The `token.txt` file will be downloaded according to your browser settings.

   > ⚠️ **CAUTION: Keep a copy of the enrollment token until the agent has been successfully enrolled. The token file will be automatically removed after each enrollment attempt (including failed attempts).**

2. Add the `token.txt` file to the unzipped folder downloaded as part of downloading an agent. For more information, see the following instructions depending on the type of agent being installed:

   - Downloading a Windows agent
   - Downloading a Mac agent
   - Downloading a Linux agent

Re-enrolling an installed agent

Once the agent has been successfully enrolled, the **Safeguard Disconnected Asset Agent** will be installed under the service account along with a **ConnectForSafeguardAssets** certificate that is valid for 60 days. The agent will automatically attempt to renew the certificate after 30 days have passed since the last certificate was issued. However, if an agent is unable to re-enroll and the certificate expires, the re-enroll command can be used to re-enroll the agent.

To re-enroll an agent

1. Download a new agent enrollment token. For more information, see Downloading an Agent Enrollment token

2. Add the new agent enrollment token to the asset. For example, re-enrolling a Windows agent requires the new token be added to the `ConnectForSafeguardWindowsAgent` folder.

   > ⚠️ **CAUTION: Keep a copy of the enrollment token until the agent has been successfully re-enrolled. The token file will be automatically removed after each enrollment attempt (including failed attempts).**

3. Open a Command Prompt or PowerShell session.

4. Run the `reenroll` command on `ConnectForSafeguardAssetsAgent`.

Removing an installed agent

The following instructions are for removing a previously installed agent. This will only remove the agent from the asset, no changes will be made to Safeguard for Privileged Passwords.

To remove an installed agent

1. On the asset the agent is installed, open a Command Prompt or PowerShell session.

2. Run the `Remove` command on `ConnectForSafeguardAssetsAgent`.

   Once the agent has been removed, you can either remove any corresponding assets within Safeguard for Privileged Passwords or enroll a new token (for more information, see Downloading an Agent Enrollment token).

Collaborators

Introduction to Collaborators

Connect for Safeguard Assets allows users to add collaborators to their service. Adding additional collaborators is optional and can be done at any time using the Collaborators page.

Collaborators page

The **Collaborators** page is displayed when **Collaborators** is clicked in the navigation bar. The **Collaborators** page is used for adding and managing the collaborators currently associated with the Connect for Safeguard Assets service.

The following options appear on this page:

Invite Collaborator

Clicking this button opens the **Invite Collaborator** dialog so you can add new collaborators to your Connect for Safeguard Assets service. For more information, see Adding additional collaborators.

🔍

This field is used to search for a user based on their name or email. To use the search functionality, start typing in the field. The table will automatically update to display results that match.

The following information and options appear in the table on this page:

Name

This displays the name specified in the collaborator invite.

Email

> This displays the email address associated with the collaborator.

Status

> This displays the status of the collaborator. When a collaborator is added they will be marked as **Invited** until the invitation has been accepted, at which point the **Status** column will update to display **Registered**. If an Administrator has selected to remove a collaborator, a status of **Pending Removal** will appear until the request has been approved or rejected.

The ⋮ button appearing for a collaborator contains the following options depending on the current status of the collaborator.

- **Remove Collaborator**: Available for a confirmed collaborator, select this option to remove the collaborator from Connect for Safeguard Assets.For more information, see Removing collaborators.

- **Re-send Invitation**: Available for an invited collaborator, selecting this option re-sends the invitation to the selected collaborator if they have not yet accepted. For more information, see Re-sending collaborator invitation.

- **Cancel Invitation**: Available for an invited collaborator, selecting this option cancels the invitation to the selected collaborator if they have not yet accepted. For more information, see Canceling collaborator invitation.

NOTE: You are unable to manage your own collaborator account.

Managing collaborators

The following sections provide information on managing collaborators for the service.

- Adding additional collaborators
- Removing collaborators
- Re-sending collaborator invitation
- Canceling collaborator invitation

Adding additional collaborators

Collaborators are optional and can be added at any time.

To add additional collaborators

1. On the **Collaborators** page, click **Invite Collaborator**.

2. In the **Invite Collaborator** dialog, enter the name and email address for the new collaborator.

3. Click **Invite**.

4. An email will be sent with a link to either register a new account that has access to your organization or, if the recipient has already registered with Starling using this email address, a notification that they now have access to your organization's Connect for Safeguard Assets service. They will be marked as **Registered** (already registered users) or **Invited** (new Starling users) until the invitation has been accepted (at which point the **Status** column will update to display **Registered**).

   NOTE: Until an invite has been accepted, the following options are available:

   - **Resend Invitation**: Selecting this option will resend the invitation.
   - **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled; however, when logging in they will be unable to access the service.

Removing collaborators

If a collaborator is no longer needed, you can remove them from the Connect for Safeguard Assets service.

NOTE: You are unable to manage your own collaborator account.

To remove collaborators

1. On the **Collaborators** page, locate the user you want to delete as a collaborator.

2. Once you have located the collaborator to edit, click the ⋮ button associated with their account.

3. Select **Remove Collaborator**.

4. In the confirmation dialog, click **Yes** to remove their access to your subscription of Connect for Safeguard Assets.

Re-sending collaborator invitation

If an invited collaborator has not accepted their invitation or their invitation was deleted, you can re-send the email invitation.

To resend collaborator invitations

1. On the **Collaborators** page, locate the invited collaborator you will be resending an invitation to.

2. Once you have located the collaborator, click the ⋮ button associated with their account.

3. Select **Re-send Invitation**.

   A new invitation will be sent to the collaborator.

Canceling collaborator invitation

If an invited collaborator is no longer needed, you can rescind their collaborator invitation from the Connect for Safeguard Assets service before they accept the emailed invitation.

To cancel collaborator invitations

1. On the **Collaborators** page, locate the invited collaborator whose invitation you will be canceling.

2. Once you have located the collaborator, click the ⋮ button associated with their account.

3. Select **Cancel Invitation**.

4. In the confirmation dialog, click **OK** to remove their access to your subscription of Connect for Safeguard Assets.

   The previously invited user will not be notified that the invitation was canceled; however, when logging in they will be unable to access the service.

Agents page

This page is used to monitor configured agents. Each agent is listed in the table on this page and contains information related to the agent's configuration and status.

Filter

Use this field to filter the data in the table based on the criteria entered in the field.

The following information about configured agents is contained in the table on this page. Clicking an agent in the table will show additional information about the agent history (for example; **Agent History**, **Agent Tasks**, and **Agent Certificate**).

Table 3: Agents table

Column	Description
Host Name	This is the name of the host the agent is installed on.
Host Type	This is the type of host the agent is installed on.
Tasks	This is the number of pending or completed tasks in the supervisor.
History	This is the number of history records. Every time the agent is updated a new record is created (up to 30 events are stored).
Certificate Expiry Days	Number of days until the agent's certificate expires. A negative value in this column is the number of days since the agent's certificate expired.
AgentId	This is the ID of the agent seen in Safeguard for Privileged Passwords.
Agent Ip	This is the IP address of the installed agent.
Service Account	This is the name of the service account used for enrollment.

Column	Description
Agent Version	This is the version of the agent installed on the host.
Date Created	This is the date the agent was created.
Time Stamp	This is the last time the properties of the agent were updated (such as version, IP, host name, etc.).

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