One Identity Safeguard Remote Access

Administration Guide

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 website (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/trademark-information.aspx. 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.**

SRA Administration Guide
Updated - 08 February 2024, 15:02

For the most recent documents and product information, see Online product documentation.

Contents

Introduction

Intended audience

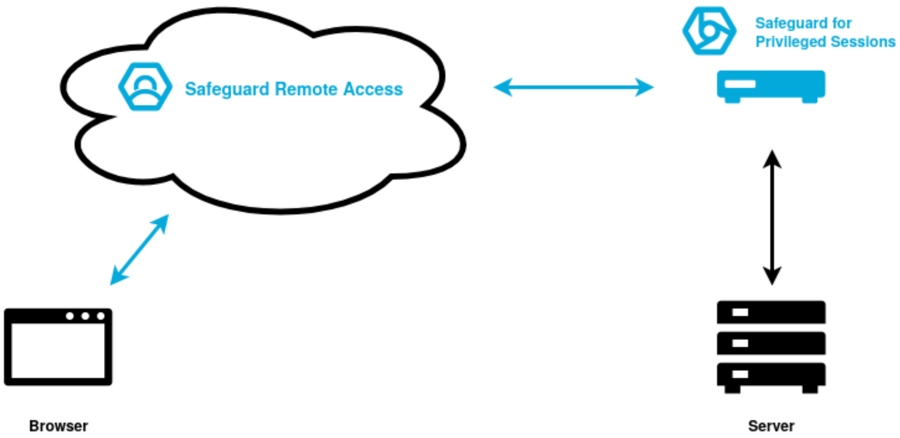
For **Administrators**, the Administration Guide contains information about how to set up One Identity Safeguard Remote Access (SRA) in One Identity Starling and how to integrate with One Identity Safeguard for Privileged Sessions (SPS).

For **Users**, the Administration Guide describes the usage and features of SRA.

Overview

SRA is a Cloud Software as a Service (SaaS) that provides a client-less, browser-based secure terminal access to servers via integration with the SPS product.

Figure 1: SRA architecture overview



Prerequisites

To use One Identity Safeguard Remote Access (SRA), you must meet the following prerequisites:

- You are using an official One Identity-supported feature or LTS version of SPS. For more information, see Version-related limitations.
- Basic network configuration is completed, and the web administrative interface is available.
- A SPS Authentication and Authorization plugin (AA plugin) is selected. For more information, see Using plugins on page 60.
- You have **Administrator** role under the SRA product in One Identity Starling.

Limitations

This section introduces the limitations of One Identity Safeguard Remote Access (SRA).

Version-related limitations

One Identity strongly recommends that you use either of the following SPS product versions:

- The latest One Identity-supported feature version.
- The latest One Identity-supported LTS version.

For more information about the latest One Identity-supported SPS feature and LTS versions, see the SPS Product Life Cycle table.

> NOTE: SPS version 6.9.n CC is no longer supported.

Security-related limitations

- End users are not required to periodically reauthenticate to a running session. Instead, once an end user logged in to a terminal session, they stay logged in to SRA.
- The bandwidth usage of terminal connections is not limited.

Functionality-related limitations

- Use Chrome-based browsers for the best user experience. Other browsers are supported on a best effort basis.
- SRA provides full support for SSH and RDP protocols only.
- No RDP remote application is supported at this time.
- Only fixed and inband destination selection defined in One Identity Safeguard for Privileged Sessions (SPS) will be picked up by SRA.
- SPS nodes are not monitored. If SPS fails or unjoins from One Identity Starling, the related target connections remain visible on SRA.
- Some browser keyword shortcuts (for example, **Ctrl+T** and **Ctrl+Shift+N**) are not forwarded to the terminal session.
- For Apple users, copy-pasting text in an active RDP remote session with **Cmd+C** and **Cmd+V** keyboard shortcuts does not work. Use ⧉ (**Copy to clipboard**) and 📋 (**Paste**) on the control panel of the session window to copy-paste text to or from the server.
- The following limitations apply to the file transfer functionality:

- SSH file transfer in active remote sessions is not supported on touch devices.
- File transfer interworking (**Cancel**, **Pause** and **Resume**) is applicable only to Chromium-based browsers (recommended: Google Chrome).

Getting started

This section and its subsections describe how to set up One Identity Safeguard Remote Access (SRA) from an Administrator point of view.

Before you can start using SRA, first you have to create a One Identity Starling account. After that, you must access One Identity Safeguard for Privileged Sessions (SPS) to perform preliminary configurations, for example, configuring the authentication and authorization plugin, creating local credential stores, setting up connection and usermapping policies and so on.

Creating and signing in to a One Identity Starling account

This section describes the process of creating and signing in to a One Identity Starling account.

One Identity Starling requires you to have a One Identity Starling organization and account to access the services.

Once you have created and accessed an organization and account, the title bar is used to manage them.

Creating a new organization

To begin using One Identity Starling and its associated services, you must first create an organization.

To create an organization and account

1. Open the One Identity Starling site (https://www.cloud.oneidentity.com/).
2. From the One Identity Starling home page, click **TRY STARLING**.
3. Select which data center you would like to access: **United States** (for the United States data center) or **European Union** (for the European Union data center).
4. Review the legal notice and to accept the use of cookies, click **Accept**. This will allow One Identity Starling to store your information for future logins.
5. In the **Email address** field, enter the email address that will be associated with the account. The email address must be less than 64 characters for the local part and for each domain part (the full email must be less than 255 characters). You need access to the specified email account to complete your registration and any future

communications regarding your organization and account will be sent to this email address.

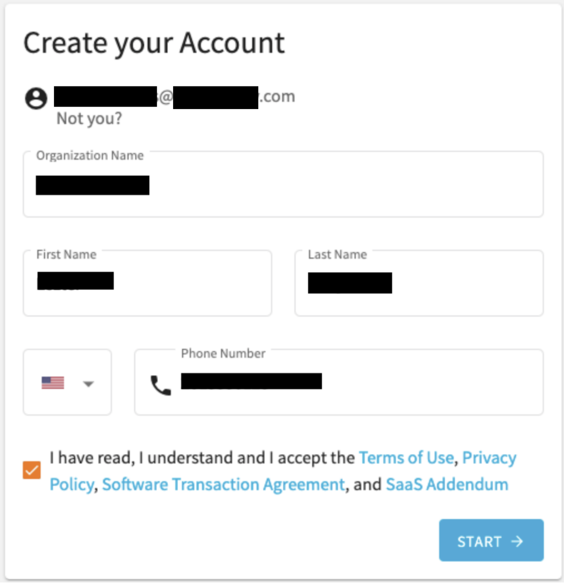
> NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center to reselect your data center region. This will restart the process for storing your login information.

6. Click **Next**.

> NOTE: At this point, One Identity Starling checks whether your email address belongs to a fully configured Azure AD work account. If that is the case, some of the following steps might be different.
>
> If you have an Azure AD tenant registered but not fully configured, you will need to use an account not dependent upon Azure AD when signing up for One Identity Starling.

7. In the **Organization Name** field, enter the name of your organization (up to 100 characters long).

Figure 2: Try Starling - Creating your account



Create your Account

[redacted]@[redacted].com

Not you?

Organization Name: [redacted]

First Name: [redacted]

Last Name: [redacted]

Phone Number: [redacted]

☑ I have read, I understand and I accept the Terms of Use, Privacy Policy, Software Transaction Agreement, and SaaS Addendum

8. In the **First Name** field, enter the first name of the account holder (up to 64 characters long).
9. In the **Last Name** field, enter the last name of the account holder (up to 64 characters long).
10. In the **Create Password** field, enter a password for your account. The password must consist of 8 to 16 characters and include three of the following items: uppercase letter, lowercase letter, number, or symbol.
11. Enter a phone number for the account.
12. Read through the Terms of Use, Privacy Policy, Software Transaction Agreement, and SaaS Addendum. If you agree, select the check box.

13. To send a verification email, after entering all your information and accepting the terms and conditions, click **START**. It could take a few minutes for the email to appear in your inbox.
14. Once the verification email has arrived, click the **Complete your registration** link within the email to open the login page of One Identity Starling.
15. Enter your credentials to access One Identity Starling.

Signing in to One Identity Starling

The following procedure applies to users that are accessing a One Identity Starling account not associated with an existing work account.

To sign in to One Identity Starling

1. From the One Identity Starling home page (https://www.cloud.oneidentity.com/), click **Sign in to Starling**.
2. The next steps will depend on whether or not you have previously stored login information.
    - If signing in to One Identity Starling using a browser that has **not previously stored your login information**:
        1. Select which data center you would like to access: **United States** (for the United States data center) or **European Union** (for the European Union data center).
        2. Review the legal notice and accept the use of cookies by clicking **Accept**. This will allow One Identity Starling to store your information for future login attempts.
        3. Enter your email address, then select **Next**.

            > NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center to reselect your data center region. This will restart the process for storing your login information.

        4. To sign in to One Identity Starling, enter your password, then click **SIGN IN**.
    - If signing in to One Identity Starling using a browser that has **previously stored your login information**:
        1. Review your email address and region, then select Next.

            > NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center to reselect your data center region. This will restart the process for storing your login information.

        2. Once One Identity Starling has confirmed there is no work account associated with your email address, a password prompt will appear. FIXME: When using this snippet in-line as a snippetText there is no new

line between the two paragraphs. Solution: Split this snippet into two snippets.To sign in to One Identity Starling, enter your password, then click **SIGN IN**.

DNS connectivity requirements for Starling products

One Identity Safeguard Remote Access (SRA) uses the following DNS names to connect and integrate with One Identity Starling products:

For SRA web interface and default HTTP settings:

- `remote-access.cloud.oneidentity.com`
- `remote-access.cloud.oneidentity.eu`

For SRA public API, which is required for One Identity Safeguard for Privileged Passwords (SPP) and One Identity Safeguard for Privileged Sessions (SPS) integration:

- `remote-access-api.cloud.oneidentity.com`
- `remote-access-api.cloud.oneidentity.eu`

NOTE: All endpoints are accessible only through HTTPS and at port `443`.

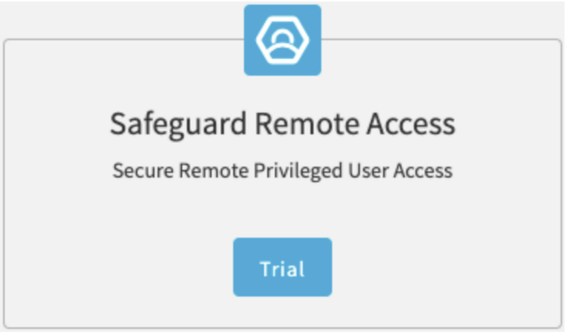
Starting the One Identity Safeguard Remote Access trial

To try and evaluate One Identity Safeguard Remote Access, you can start a trial from the One Identity Starling home page.

To start the One Identity Safeguard Remote Access trial

1. From the One Identity Starling home page (https://www.cloud.oneidentity.com/), click **Sign in to Starling**.
2. Navigate to **Services**.
3. Under **Starling Remote Access**, click **Trial**

Figure 3: Services > Trial - Starting the One Identity Safeguard Remote Access trial



4. Select **Your Location** and click **Confirm**.

   The One Identity Safeguard Remote Access trial appears under your **My Services** list. You can monitor your trial expiration date here.

5. Click the One Identity Safeguard Remote Access trial.

Configure One Identity Safeguard for Privileged Sessions

This section describes the various settings and policies that you must configure in One Identity Safeguard for Privileged Sessions (SPS) to join the appliance to One Identity Starling and integrate with One Identity Safeguard Remote Access (SRA).

The configuration pages referenced in this section are applicable to the web interface of SPS and are written in bold. For example, **Basic Settings** > **Network**.

- Configuring Usermapping policy
- Configuring a Credential store
- Upload Authentication and Authorization plugin
- Configuring Authentication and Authorization plugin
- Configuring a connection policy
- HTTPS proxy
- Joining SPS to Starling
- Enabling One Identity Safeguard Remote Access

Configuring Usermapping policy

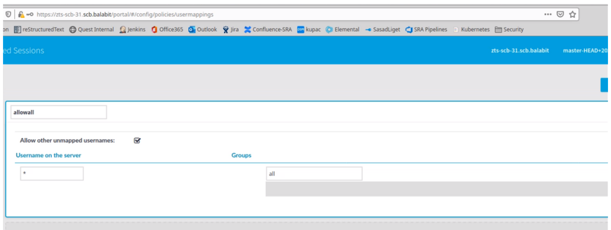
In a typical One Identity Safeguard Remote Access (SRA) use case, the end-user and the user on the (target) server are different. The end-user is identified by their email address and the server user is typically identified by an administrative account name like `root` or `Administrator`. One Identity Safeguard for Privileged Sessions (SPS) does not allow different end-user (called gateway user in SPS) and server user by default in a connection. Therefore, you must apply a Usermapping policy on the Connection policy.

To create a new Usermapping policy

1. Navigate to **Policies** > **Usermapping policies**.
2. Add a new policy (**Username on the server** and **Groups**).

> **Example: Creating a new Usermapping policy**
>
> As an example, the following policy allows any kind of user mapping.
>
> - **Username on the server**: *
> - **Group**: `all`

Figure 4: Policies > Usermapping policies - Creating usermapping policies



https://zts-scb-31.scb.balabit/portal/#/config/policies/usermappings

allowall

Allow other unmapped usernames: ☑

Username on the server	Groups
*	all

For more information on HTTPS proxy setting, refer to the One Identity Safeguard for Privileged Sessions Administration Guide or part of it in Configuring usermapping policies on page 54 in the Appendix.

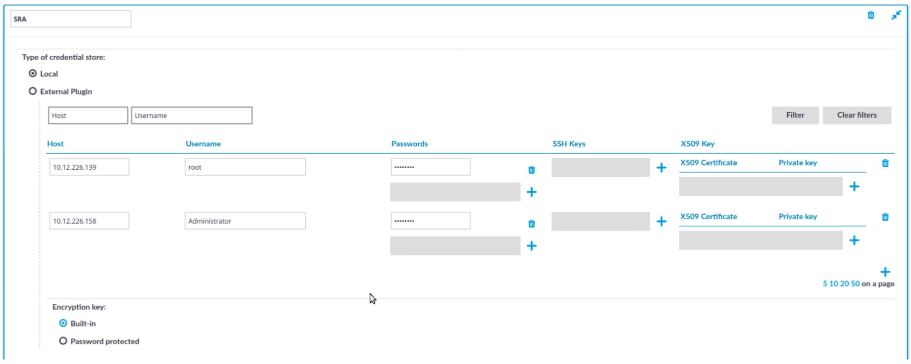
Configuring a Credential store

Configuring a credential store is an optional step for both RDP and SSH connection policies.

To enable password-less login to target servers

1. Create a local credential store.
2. Setup login credentials to the target server.

Figure 5: Policies > Credential stores — Creating local credential stores



SRA

Type of credential store:

● Local

○ External Plugin

Host | Username | Filter | Clear filters

Host	Username	Passwords	SSH Keys	X509 Key
10.12.226.139	root	••••••••		X509 Certificate / Private key
10.12.226.158	Administrator	••••••••		X509 Certificate / Private key

5 10 20 50 on a page

Encryption key:

● Built-in

○ Password protected

For more information on HTTPS proxy setting, refer to the One Identity Safeguard for Privileged Sessions Administration Guide or part of it in Configuring local Credential Stores on page 56 and Using credential stores for server-side authentication on page 59 in the Appendix.

Upload Authentication and Authorization plugin

An Authentication and Authorization (AA) plugin must be used in One Identity Safeguard for Privileged Sessions (SPS) connection policies that are intended for use with One Identity Safeguard Remote Access (SRA).

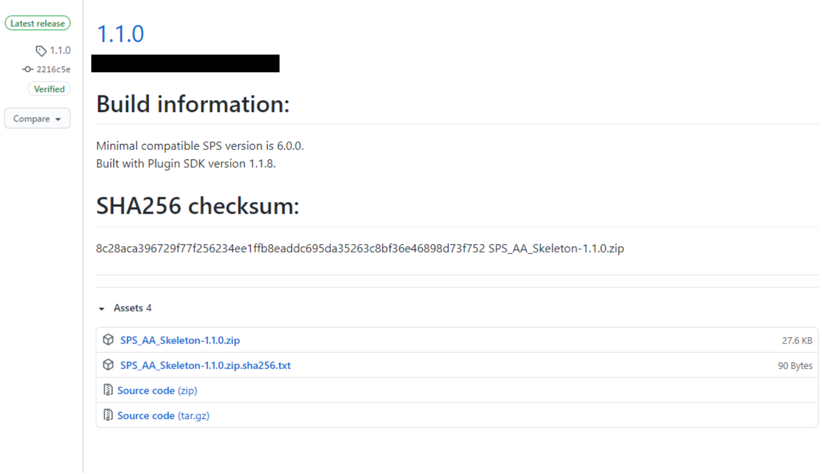
In the SRA use case, the authentication of the end-user is performed on the web when the end-user navigates to remote-access.cloud.oneidentity.com. In SPS terminology, the end-user authentication is called gateway authentication. Gateway authentication is required to be able to audit the end-user. SPS can delegate the gateway authentication to SRA, if a suitable AA plugin is in use.

There are two options:

- Use a **dummy AA plugin** that does nothing and delegates gateway authentication fully to the cloud:

  https://github.com/OneIdentity/safeguard-sessions-plugin-skeleton-aa/releases/tag/1.1.0

Figure 6: Downloading the AA plugin



1.1.0

[redacted]

Build information:

Minimal compatible SPS version is 6.0.0.
Built with Plugin SDK version 1.1.8.

SHA256 checksum:

```
8c28aca396729f77f256234ee1ffb8eaddc695da35263c8bf36e46898d73f752 SPS_AA_Skeleton-1.1.0.zip
```

Assets 4

SPS_AA_Skeleton-1.1.0.zip	27.6 KB
SPS_AA_Skeleton-1.1.0.zip.sha256.txt	90 Bytes
Source code (zip)	
Source code (tar.gz)	

Download the first `.zip` file.

- Use an **official AA plugin** that performs Multi-Factor Authentication:

  https://support.oneidentity.com/one-identity-safeguard-for-privileged-sessions/6.8.1/download-new-releases?filterType=software&filterValue=Plugins

  Alternatively, download from Github (not officially supported):

  https://github.com/search?q=topic%3Aoi-sps-plugin+org%3AOneIdentity

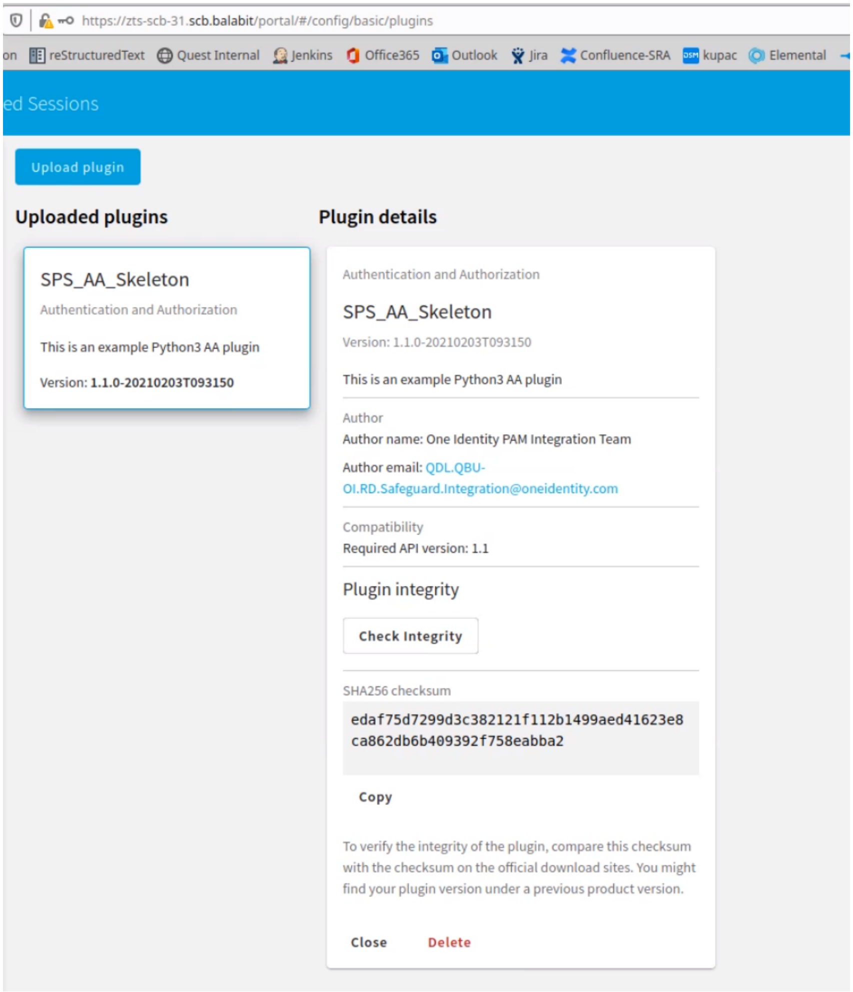
> NOTE: Official plugins are built with an open source Plugin SDK: https://pypi.org/project/oneidentity-safeguard-sessions-plugin-sdk/

Uploading the plugin

1. Navigate to **Basic Settings** > **Plugins**.
2. Click **Upload plugin**.

   Expected outcome: The plugin that you have uploaded is displayed:

Figure 7: Uploading the plugin


https://zts-scb-31.scb.balabit/portal/#/config/basic/plugins
on reStructuredText Quest Internal Jenkins Office365 Outlook Jira Confluence-SRA kupac Elemental
ed Sessions
Upload plugin

Uploaded plugins

SPS_AA_Skeleton

Authentication and Authorization

This is an example Python3 AA plugin

Version: 1.1.0-20210203T093150

Plugin details

Authentication and Authorization

SPS_AA_Skeleton

Version: 1.1.0-20210203T093150

This is an example Python3 AA plugin

Author

Author name: One Identity PAM Integration Team

Author email: QDL.QBU-OI.RD.Safeguard.Integration@oneidentity.com

Compatibility

Required API version: 1.1

Plugin integrity

Check Integrity

SHA256 checksum

```
edaf75d7299d3c382121f112b1499aed41623e8
ca862db6b409392f758eabba2
```

Copy

To verify the integrity of the plugin, compare this checksum with the checksum on the official download sites. You might find your plugin version under a previous product version.

Close Delete

For more information on the HTTPS proxy setting, see the One Identity Safeguard for Privileged Sessions Administration Guide or part of it in Using plugins on page 60 in the Appendix.

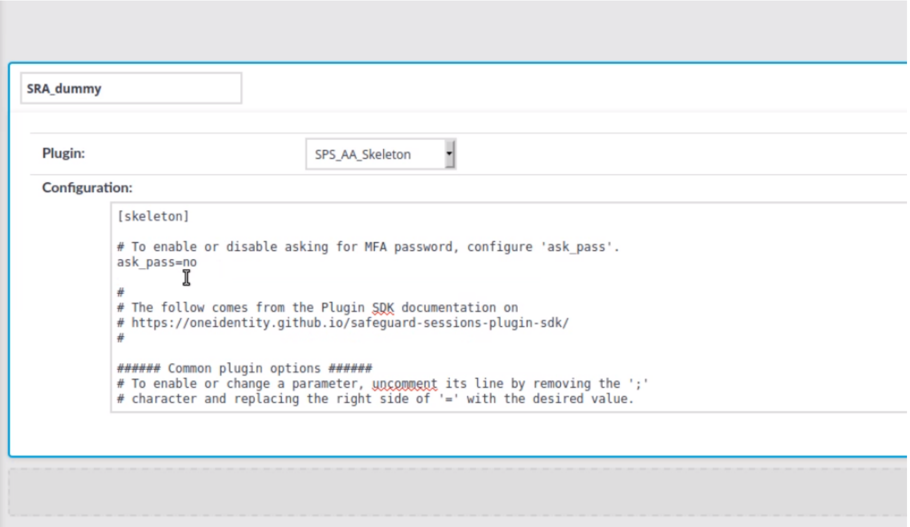
Configuring Authentication and Authorization plugin

To configure the AA plugin

1. Navigate to **Policies** > **AA plugin configurations**.
2. Create a new configuration item and configure the selected plugin.

The following example is applicable if you downloaded the dummy **`SPS_AA_skeleton`** plugin:

Figure 8: SPS_AA_skeleton plugin



SRA_dummy

Plugin: SPS_AA_Skeleton

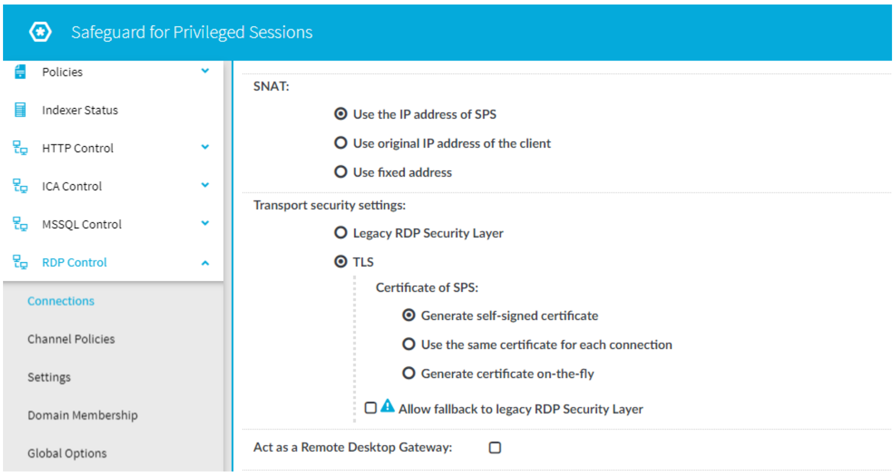
Configuration:

```
[skeleton]

# To enable or disable asking for MFA password, configure 'ask_pass'.
ask_pass=no

#
# The follow comes from the Plugin SDK documentation on
# https://oneidentity.github.io/safeguard-sessions-plugin-sdk/
#

###### Common plugin options ######
# To enable or change a parameter, uncomment its line by removing the ';'
# character and replacing the right side of '=' with the desired value.
```

Configuring a connection policy

Create connection policies for RDP and SSH connections as needed. The connection policies define what is reachable via the One Identity Safeguard for Privileged Sessions appliance and what policies are enforced.

> NOTE: When creating RDP connections in SPS, the checkbox for the **Act as a Remote Desktop Gateway** functionality must be left empty, as SRA does not support the usage of RDP gateways.
>
> **Figure 9: RDP Control > Connections > Act as a Remote Desktop Gateway - Disabling the Remote Desktop Gateway functionality**



SNAT:
- ● Use the IP address of SPS
- ○ Use original IP address of the client
- ○ Use fixed address

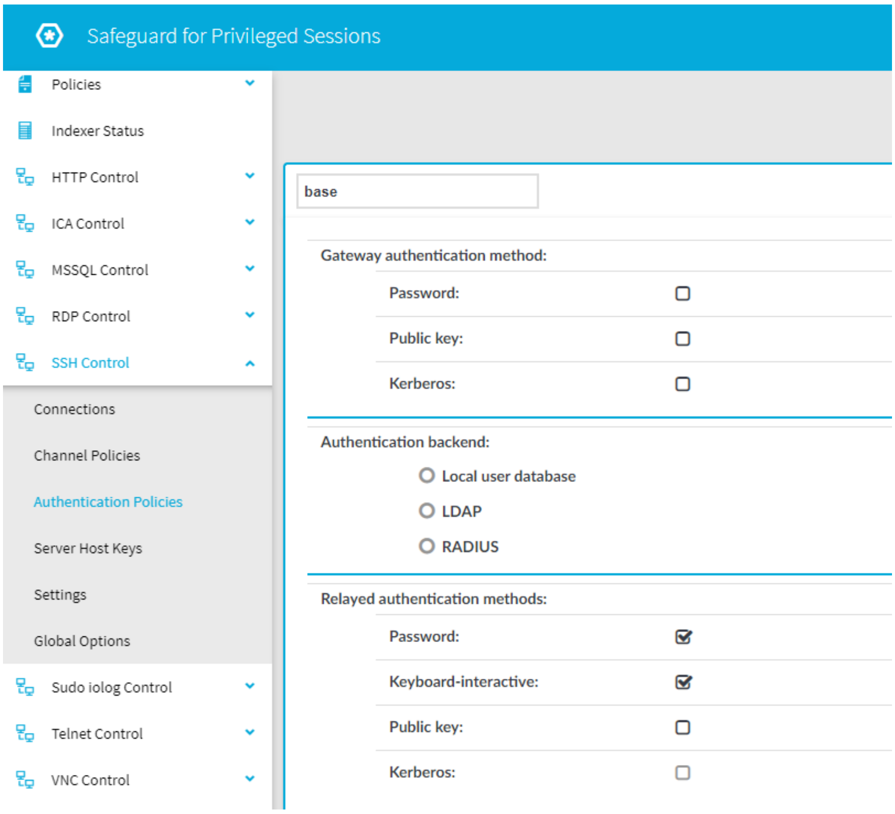
Transport security settings:
- ○ Legacy RDP Security Layer
- ● TLS
  - Certificate of SPS:
    - ● Generate self-signed certificate
    - ○ Use the same certificate for each connection
    - ○ Generate certificate on-the-fly
  - □ Allow fallback to legacy RDP Security Layer

Act as a Remote Desktop Gateway: □

For more information about RDP gateways, see *Using One Identity Safeguard for Privileged Sessions (SPS) as a Remote Desktop Gateway* in the One Identity Safeguard for Privileged Sessions Administration Guide.

NOTE: When creating SSH connections, the authentication policy must not include gateway authentication.

Figure 10: SSH Control > Authentication Policies > Gateway authentication method - All possible options (Password, Public key, and Kerberos) must be left unchecked



base

Gateway authentication method:

Password: □

Public key: □

Kerberos: □

Authentication backend:

○ Local user database

○ LDAP

○ RADIUS

Relayed authentication methods:

Password: ☑

Keyboard-interactive: ☑

Public key: □

Kerberos: □

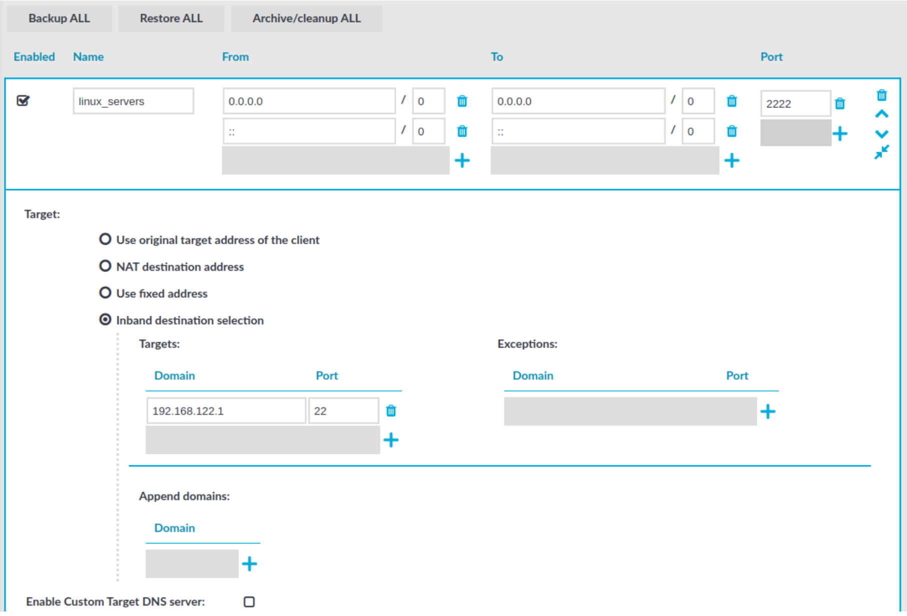
For more information, see *Client-side authentication settings* in the One Identity Safeguard for Privileged Sessions Administration Guide.

Some parameters have special meaning and requirements regarding One Identity Safeguard Remote Access (SRA).

Name

The name of the connection policy will be displayed on the SRA **Connections** page. The name appears on the connection tiles if the target of the connection policy is a fixed address. In case of inband target selection, the name is displayed below a horizontal separator line and becomes the name of the group of targets reachable via this connection policy. In the example, `linux_servers` is the name of the connection policy:

Figure 11: Setting the name and target address of the connection policy



Enabled	Name	From	To	Port
☑	linux_servers	0.0.0.0 / 0 :: / 0	0.0.0.0 / 0 :: / 0	2222

Target:

○ Use original target address of the client

○ NAT destination address

○ Use fixed address

● Inband destination selection

Targets:

Domain	Port
192.168.122.1	22

Exceptions:

Domain	Port

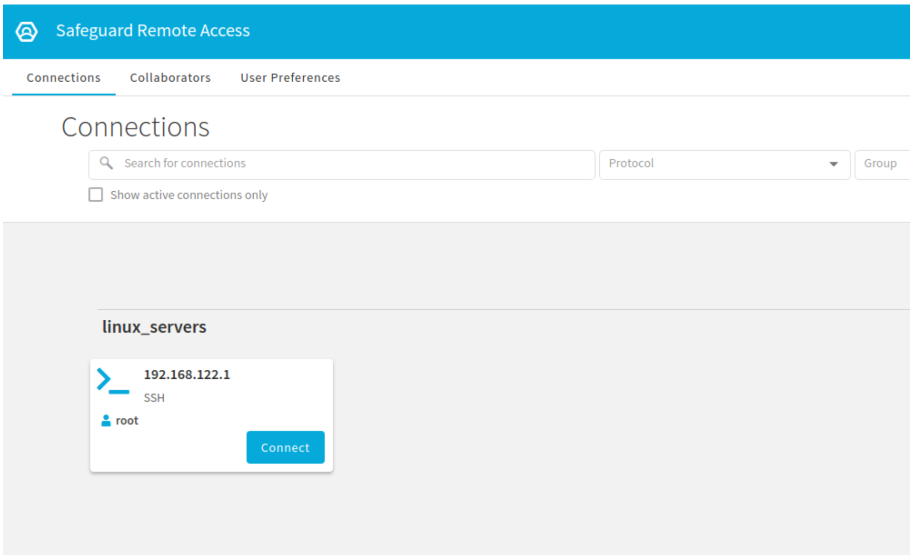
Append domains:

Domain

Enable Custom Target DNS server: □

In this example, **`linux_servers`** is the group containing one connection towards the `192.168.122.1` target.

Figure 12: Connection groups



From

The **From** parameter of the connection policy defines the IPv4 or IPv6 networks where the clients may connect from. In case of SRA, the client could be anywhere on the Internet, so to cover all IPv4 clients, fill this field with `0.0.0.0/0`.

CAUTION: To handle clients connecting from internal networks (that is, LAN or VPN) differently, you must add a similar connection policy right above the connection policy for SRA. The To and Port fields must match and the From field should specify the internal network, for example, `10.0.0.0/8` or similar. This is especially useful when introducing a different kind of (gateway) authentication for locally connected clients that bypass SRA.

To

The **To** parameter specifies what address the clients make requests to. In the case of SRA, set this also to `0.0.0.0/0` to enable the automated handling of this parameter.

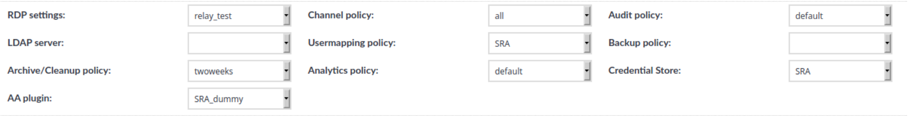
Target

Only the options **`Use fixed address`** and **`Inband destination selection`** are compatible with SRA. In case of inband destination selection, the connection tiles will display only the target domains that either specify specific IPv4 or IPv6 addresses, or contain a hostname. Subdomains and networks are ignored.

Policies

Use the configuration for AA plugin (Configuring Authentication and Authorization plugin), credential store (Configuring a Credential store) and usermapping policy (Configuring Usermapping policy) that you have previously created while you were configuring SPS. Every other configuration can be left either on default or be defined by the user.

Figure 13: Connection policy settings



RDP settings:	relay_test	Channel policy:	all	Audit policy:	default
LDAP server:		Usermapping policy:	SRA	Backup policy:	
Archive/Cleanup policy:	twoweeks	Analytics policy:	default	Credential Store:	SRA
AA plugin:	SRA_dummy				

For more information on the HTTPS proxy setting, see the One Identity Safeguard for Privileged Sessions Administration Guide or part of it in Configuring connections on page 60 in the Appendix.

HTTPS proxy

One Identity Safeguard for Privileged Sessions requires an HTTPS access to One Identity Safeguard Remote Access in the cloud. If the One Identity Safeguard for Privileged Sessions appliance has no direct connectivity to the Internet (for example, it is behind a firewall), you can configure a HTTPS proxy in **Basic Settings** > **Network** configuration page.

For more information on the HTTPS proxy setting, see the One Identity Safeguard for Privileged Sessions Administration Guide, or to the relevant part of it in HTTPS proxy on page 65 section of the Appendix.

Joining SPS to Starling

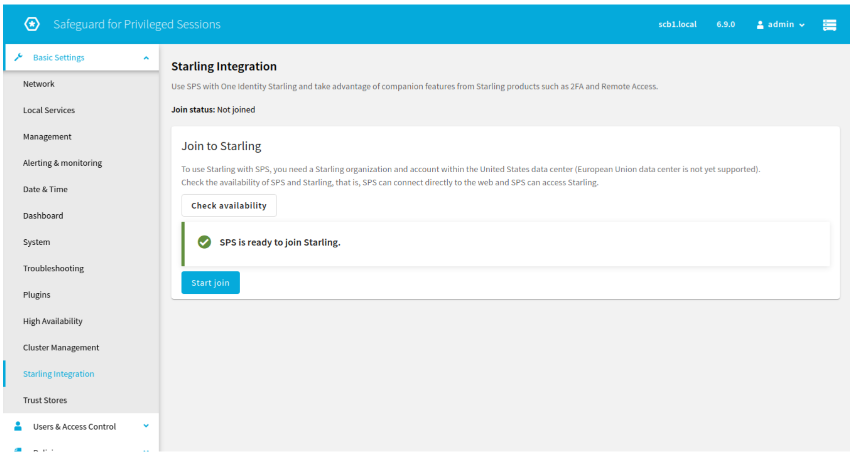
Join the One Identity Safeguard for Privileged Sessions (SPS) appliance to One Identity Starling. This enables the appliance to integrate with One Identity Safeguard Remote Access (SRA) and share data.

To join SPS to One Identity Starling

1. Navigate to **Basic Settings** > **Starling Integration** > **Join to Starling**.
2. Click **Start join** and follow the instructions.

   NOTE: If asked, select the United States data center.

Figure 14: Join SPS to One Identity Starling



Starling Integration

Use SPS with One Identity Starling and take advantage of companion features from Starling products such as 2FA and Remote Access.

Join status: Not joined

Join to Starling

To use Starling with SPS, you need a Starling organization and account within the United States data center (European Union data center is not yet supported).
Check the availability of SPS and Starling, that is, SPS can connect directly to the web and SPS can access Starling.

Check availability

✓ SPS is ready to join Starling.

Start join

For more information on the HTTPS proxy setting, see the One Identity Safeguard for Privileged Sessions Administration Guide, or the relevant part of it in Joining SPS to One Identity Starling on page 66 in the Appendix.

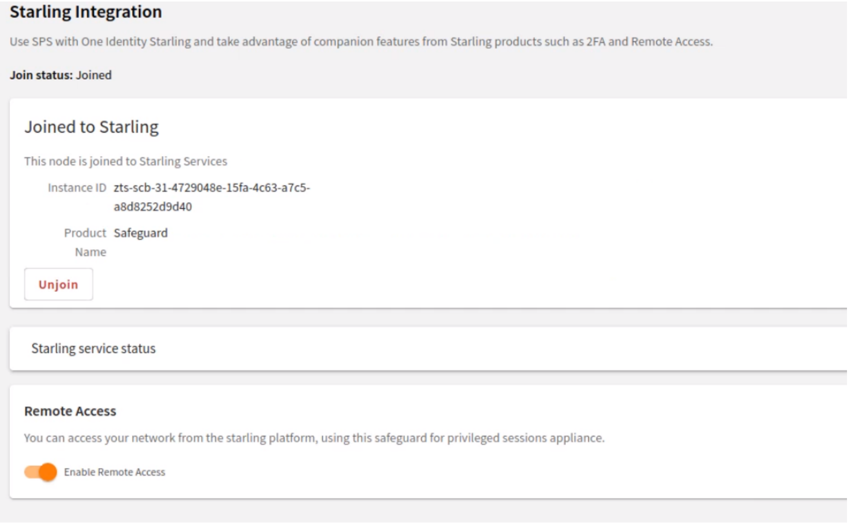
Enabling One Identity Safeguard Remote Access

One Identity Safeguard Remote Access must be enabled manually to access connections created on One Identity Safeguard for Privileged Sessions.

To enable One Identity Safeguard Remote Access

1. Navigate to **Basic Settings** > **Starling Integration** > **Remote Access** > **Enable Remote Access**.

   Figure 15: Enable Remote Access

   Starling Integration

   Use SPS with One Identity Starling and take advantage of companion features from Starling products such as 2FA and Remote Access.

   Join status: Joined

   Joined to Starling

   This node is joined to Starling Services

   Instance ID zts-scb-31-4729048e-15fa-4c63-a7c5-a8d8252d9d40

   Product Name Safeguard

   Unjoin

   Starling service status

   Remote Access

   You can access your network from the starling platform, using this safeguard for privileged sessions appliance.

   Enable Remote Access

2. To enable One Identity Safeguard Remote Access, toggle the **`Enable Remote Access`** switch.

3. On the One Identity Safeguard Remote Access home page, your connections should now be listed with the default accounts (**`root`** for SSH and **`Administrator`** for RDP).

Administrator-side use cases

This section covers the Administrator-side use cases for One Identity Safeguard Remote Access (SRA).

Administrator web interface location

The web interface for One Identity Safeguard Remote Access is accessible on the link: remote-access.cloud.oneidentity.com.

The contents of the interface are loaded from the One Identity Safeguard Remote Access (SRA) subscription where the user is an **Administrator** or **User**. If the user is a member of multiple subscriptions, then select the appropriate subscription in the upper right corner.

Adding a new connection to an existing target server

Each target server can serve multiple connections. Connections consist of two elements:

- An asset (the target server itself).
- An account (the Azure Active Directory account).

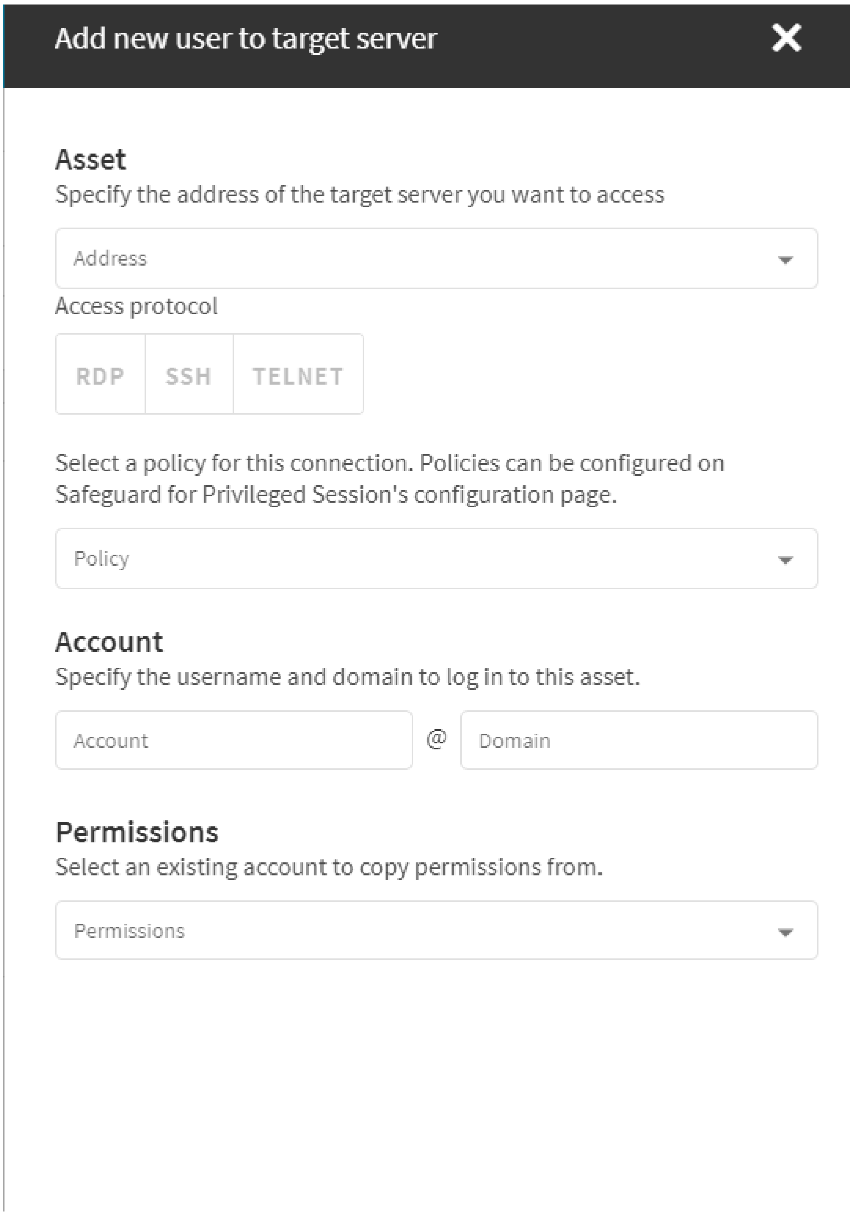
You can group these connections based on various attributes, such as the applied protocol (RDP, SSH, or TELNET), the SPS connection policy name, or the address of the target server.

> TIP: If you want to speed up adding new connections, you can import them from a CSV file. For more information, see Importing connections from a CSV file.

To add a new connection to an existing target server

1. On the **Connections** page, click **New Connection**.

   Figure 16: Connections > New Connection > Add new user to target server - Adding a new connection



Add new user to target server

Asset

Specify the address of the target server you want to access

Access protocol

Select a policy for this connection. Policies can be configured on Safeguard for Privileged Session's configuration page.

Account

Specify the username and domain to log in to this asset.

Permissions

Select an existing account to copy permissions from.

2. The **Add new user to target server** sidesheet is split into two sections as connections comprise of assets and accounts.

- For **Asset** configuration:
    1. Specify the address of the target server that you want to access.
    2. Specify the access protocol of the new connection (for example, SSH, RDP, or TELNET).
    3. Select a policy for this connection. To configure a policy in One Identity Safeguard for Privileged Sessions (SPS), navigate to **Policies**.
- For **Account** configuration:
    1. Specify a username.
    2. (Optional) Specify a domain name in which the username you specified is a member.

3. Click **Create**.

Importing connections from a CSV file

You can speed up adding your user-specific connections to the One Identity Safeguard Remote Access (SRA) **Connections** page by importing them from a CSV file.

Successfully imported connections are automatically grouped under the respective connection policies.

For information about adding new connections manually, see Adding a new connection to an existing target server.

Prerequisites

- You must have an SRA **Admin** role.
- An SPS instance joined to One Identity Starling.

Limitations

- Only CSV file format is supported for upload, with a maximum size of 10 MB.
- SRA only accepts commas as delimiters in the CSV files.
- Expected columns for the CSV files:

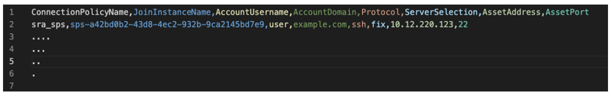
Name of column	Requirement	Accepted values
`AssetAddress`	Required	`<IPv4-address>` | `<IPv6-address>` | `hostname`
`AccountDomain`	Optional	
`AssetPort`	Required	`<nonnegative integer>`

Name of column	Requirement	Accepted values
`AccountUsername`	Required	`<string>`
`ConnectionPolicyName`	Required	`<string>`
`JoinInstanceName`	Required	`<JoinInstanceID>`
`Protocol`	Required	`rdp` | `ssh`
`ServerSelection`	Required	`fix` | `inband`

CSV file structure

You can use the expected columns and corresponding values of a CSV file in any order you prefer. The following screenshot illustrates the structure and contents of an example CSV file.

Figure 17: Example of CSV file structure and contents



```
ConnectionPolicyName,JoinInstanceName,AccountUsername,AccountDomain,Protocol,ServerSelection,AssetAddress,AssetPort
sra_sps,sps-a42bd0b2-43d8-4ec2-932b-9ca2145bd7e9,user,example.com,ssh,fix,10.12.220.123,22
....
...
..
.

```

Uploading the CSV file

When you made sure you meet the prerequisites, you can start uploading your CSV file.

To upload the CSV file that contains the connections you want to add

1. Log in to SRA as **Admin**.
2. Navigate to the SRA **Connections** page.
3. Click **Import CSV**.
4. Select the CSV file you want to upload from your computer, then click **Open**.

   At the bottom of the page, snackbar notifications indicate the current upload state.

   For example, **Successfully imported 8 connections. Refresh the page to see the results.** indicates 8 successfully imported connections.

   > ⚠ **CAUTION: If you navigate away from the page while uploading is in progress, you will not see the snackbar notifications about the progress and if the upload was successful.**

   > NOTE: While uploading the CSV file, **Import CSV** is grayed out, then enabled again after the upload is complete.

5. Refresh the UI to see the newly added connections, grouped under connection policies.

   Expected result: After refreshing the UI, the newly imported connections are displayed as tiles under the respective connection policy group on the SRA **Connections** page.

Troubleshooting

In some cases, the snackbar displays the **Successfully imported 0 connections. Refresh the page to see the results.** message.

Possible reasons:

- Your browser does not support file upload.
- The file upload functionality is switched off in your browser.
- The file upload functionality is switched on in your browser, but the file size exceeds the limit configured in your browser.
- You are trying to import the same connections that you have previously imported.
- The `JoinInstanceName` value is not valid.
- There is no connection policy with the specified `ServerSelection`, `AssetAddress`, or `AssetPort` (or any combination of them) in the SPS connection policy configuration.
- A connection has already been added with the specified `AccountUsername` and `AccountDomain`. Therefore, the connection will not be imported to the specified connection policy group.

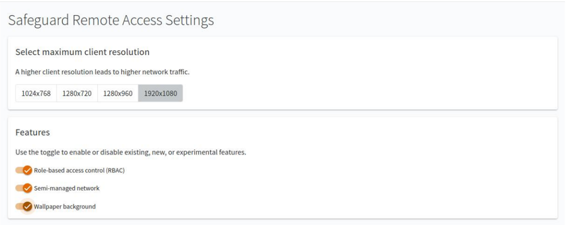
Configuring maximum client resolution

Configuring client resolution correctly results in a better stream quality.

> NOTE: A higher client resolution results in higher network traffic load.

To configure maximum client resolution

1. Click ⚙ (Settings) and select **Safeguard Remote Access Settings**.
2. Find **Select maximum client resolution**.

   Safeguard Remote Access Settings

   Select maximum client resolution

   A higher client resolution leads to higher network traffic.

   1024x768 | 1280x720 | 1280x960 | 1920x1080

   Features

   Use the toggle to enable or disable existing, new, or experimental features.

   ✓ Role-based access control (RBAC)

   ✓ Semi-managed network

   ✓ Wallpaper background

3. Select the preferred client resolution.

   The default value is **`1024x768`**.

> NOTE: If the administrator sets a client resolution as maximum, that means that the user is free to select any of the available client resolutions up until the maximum resolution. For example, if the maximum client resolution is set to **`1280x720`**, the user can still set the client resolution to **`1024x768`**, but cannot set it higher than **`1280x720`**.

Adding Azure Active Directory users directly

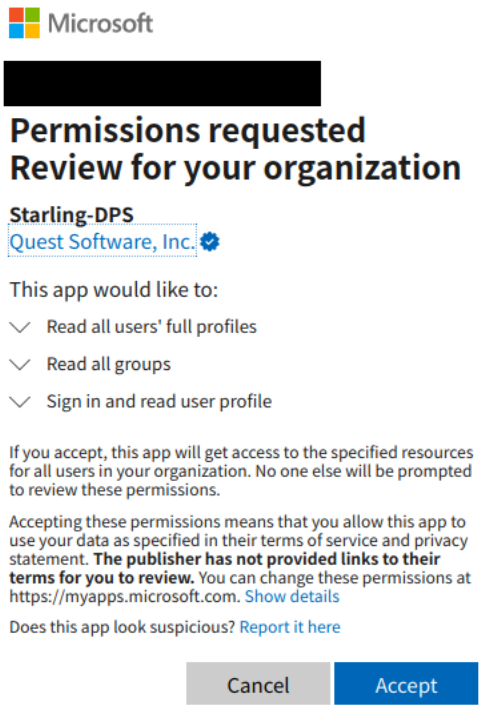
To allow your users to access specific servers through One Identity Safeguard Remote Access (SRA), add them to selected Azure Active Directory (AAD) groups. Adding Azure AD users directly to SRA simplifies the onboarding workflow, as there is no need to set up a One Identity Starling account.

With this approach, employees within an organization can visit https://remote-access.cloud.oneidentity.com, provide their Azure AD username and password and/or other credentials, and gain access to SRA connections permitted to them based on their group membership.

Prerequisites

- The employees of the organization are provisioned in Azure AD.
- There is a user with `Administrator` role in that AAD. The Administrator must consent to One Identity Starling having read-only access to Azure AD, specifically to:
  - Read all users' full profiles
  - Read all groups
  - Sign in and read user profile

Figure 18: Allow One Identity Starling to have access to your Azure Active Directory user groups



Microsoft

[redacted]

Permissions requested
Review for your organization

Starling-DPS
Quest Software, Inc.

This app would like to:

- Read all users' full profiles
- Read all groups
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

To add Azure Active Directory users directly

1. Log into One Identity Starling (https://account.cloud.oneidentity.com/) as an **Organization-administrator** and also as an Azure Active Directory **Administrator**.
2. Click ⚙ (Settings) and manage **Directory Services**.
3. Click **Register Directory** and follow the instructions.
4. Go to SRA and start setting up connections with role assignments. For more information, see Granting connection access to AAD users.
5. Enable the role-based access control (RBAC) functionality. For more information, see Enabling role-based access control.

Granting connection access to AAD users

Use role assignment to organize your users and resources into groups based on access rights.

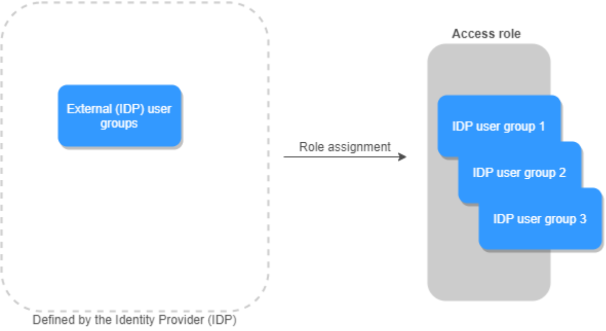
There are two ways to access One Identity Safeguard Remote Access (SRA):

- When you are an **Administrator**, you can access SRA with a One Identity Starling account.
- When you are a **User**, you can access either via your One Identity Starling account and with a **User** role, or enter with an Azure Active Directory (AAD) user account directly (as if you were a One Identity Starling user).

Access can be granted only to AAD groups, not to individual users. This can be achieved by assigning the **Access** role to AAD groups over connections. When a user logs in with AAD directly, SRA looks up their group memberships and lists only those connections where the **Access** role was assigned to one of the user's groups.

> NOTE: Role-based access control is possible only when users log in with their AAD user account directly. When users log in with their One Identity Starling account, all connections are available for connecting.

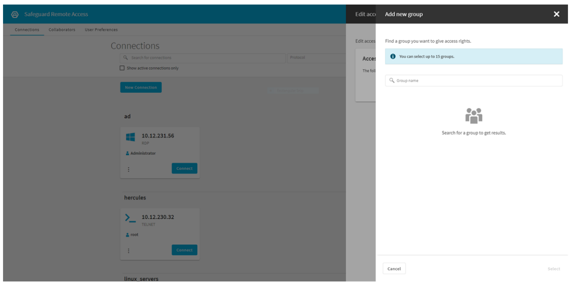
Figure 19: Role assignment - organizing user and resource groups



To assign the Access role to a new group

1. Navigate to the **Connections** page and click the ⋮ (Options) on the connection card.
2. Select **Role assignment**. The **Edit access for <IP-address-of-target-server>** side sheet will open on the right. The **Access** field displays all groups that have access to that connection.
3. Click **Add new group**. A side sheet will open.
4. Start typing a group name in the **Group name** search bar to find the groups you want to grant access rights to this connection. The search results will appear as you type (for example Group name, Group ID, Tenant ID). The search expression works both for a whole or a partial group name. You can select up to 15 groups.

Figure 20: Connection tile > ⋮ > Role assignment > Add new group — Finding your groups



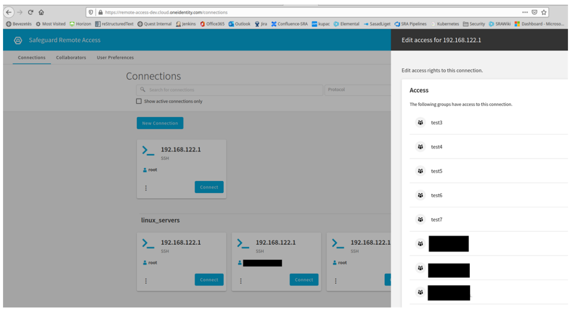
Add new group

Find a group you want to give access rights.

You can select up to 15 groups.

Search for a group to get results.

Figure 21: Connection tile > ⋮ > Role assignment > Add new group — Adding a new group



Edit access for 192.168.122.1

Edit access rights to this connection.

Access

The following groups have access to this connection.

- test3
- test4
- test5
- test6
- test7
- [redacted]
- [redacted]
- [redacted]

5. Click **Select**.

To remove role assignment for a group

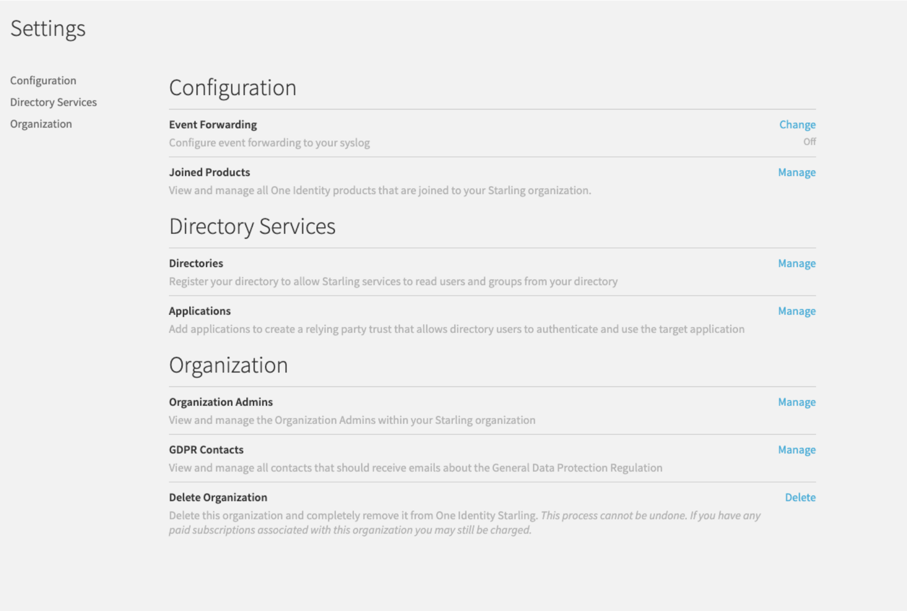
1. Find the group whose role assignment you want to remove and click the trashbin icon next to it. A confirmation dialog will appear.
2. Confirm your delete request.

Enabling role-based access control

Role-based access control (RBAC) is used to define which user groups have access to which resources and workflows in One Identity Safeguard Remote Access (SRA). RBAC is not enabled automatically when you group roles and connections in SRA. You must enable it manually.

For the RBAC functionality to work, at least one Azure Active Directory must be registered and consented under **Starling Settings** > **Manage Directories** in One Identity Starling.

Figure 22: Starling Settings > Directory Services > Manage Directories



Settings

- Configuration
- Directory Services
- Organization

Configuration

Event Forwarding — Change
Configure event forwarding to your syslog — Off

Joined Products — Manage
View and manage all One Identity products that are joined to your Starling organization.

Directory Services

Directories — Manage
Register your directory to allow Starling services to read users and groups from your directory

Applications — Manage
Add applications to create a relying party trust that allows directory users to authenticate and use the target application

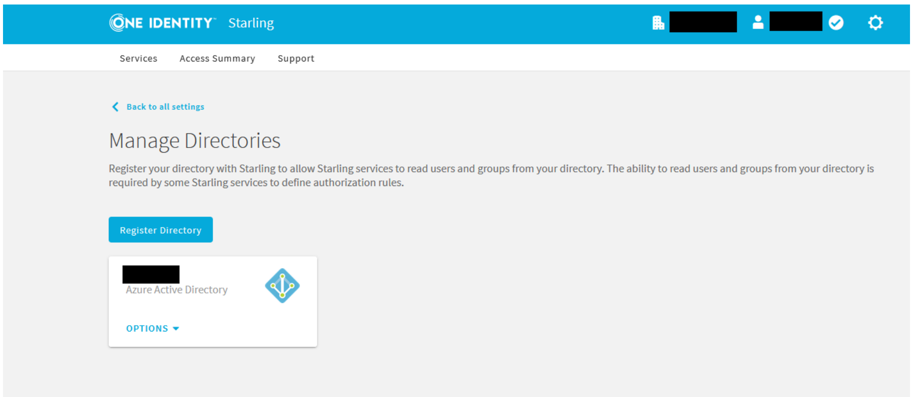
Organization

Organization Admins — Manage
View and manage the Organization Admins within your Starling organization

GDPR Contacts — Manage
View and manage all contacts that should receive emails about the General Data Protection Regulation

Delete Organization — Delete
Delete this organization and completely remove it from One Identity Starling. *This process cannot be undone. If you have any paid subscriptions associated with this organization you may still be charged.*

Figure 23: Manage Directories > Register Directory — Registering active directories to your One Identity Starling organization.



Manage Directories

Register your directory with Starling to allow Starling services to read users and groups from your directory. The ability to read users and groups from your directory is required by some Starling services to define authorization rules.

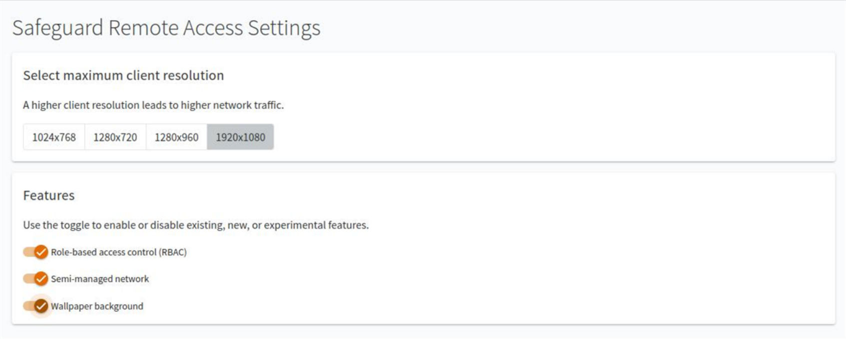
To register or remove active directories, the user must be a One Identity Starling organization admin.

If no Active Directory is registered in One Identity Starling, the role assignment functionality will be unavailable for both administrators and users. You can check this by opening the ⋮ (Options) menu of a connection card. If RBAC in unavailable, the **Role assignments** menu item will be grayed out.

> NOTE: As RBAC is a central feature, when enabled, it applies to all groups created later. When you disable RBAC, all groups governed by this feature lose access to SRA. If you want to remove access rights from certain groups, that must be done one by one.

To enable role-based access control in SRA

1. Click ⚙ (Settings) and select **Safeguard Remote Access Settings**.
2. Find **Features** > **Role-based access control (RBAC)**.



Safeguard Remote Access Settings

Select maximum client resolution

A higher client resolution leads to higher network traffic.

1024x768 | 1280x720 | 1280x960 | 1920x1080 (selected)

Features

Use the toggle to enable or disable existing, new, or experimental features.

- ✓ Role-based access control (RBAC)
- ✓ Semi-managed network
- ✓ Wallpaper background

3. Slide the toggle to enable RBAC.

NOTE: Disabling the RBAC functionality with the toggle affects only regular users. Administrators can still access RBAC functionalities when the **Role-based access control (RBAC)** toggle is disabled.

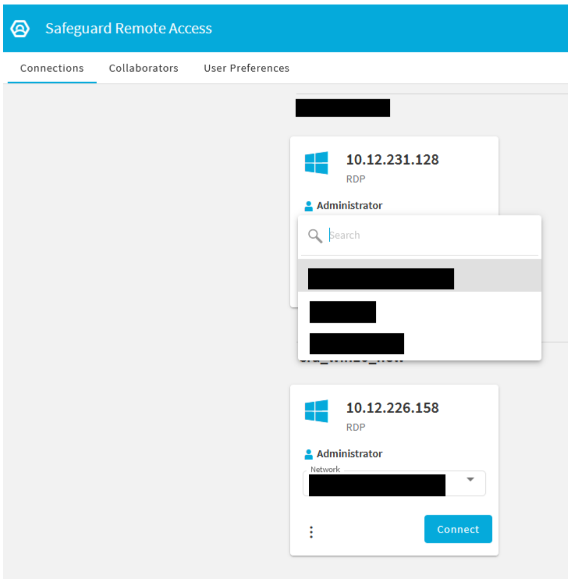
Enabling semi-managed network

Improve your network performance and latency with the semi-managed network functionality of One Identity Safeguard Remote Access (SRA). Depending on your network configuration, you may have one or multiple SPS nodes available. With semi-managed network, you can select which SPS node to use in your network when you initiate a connection.

To initiate a connection with a specific SPS node

1. Navigate to the SRA **Connections** page and find the connection tile you want to work with.
2. Open the dropdown menu of that connection tile's **Network** field and search for the name of the SPS node you want to use for initiating this connection.

Figure 24: Connections > The connection tile of your choice > Network — Selecting a SPS node for your session



> NOTE: Your selection will not be saved for future reference. You must set your preferences every time you initiate a new connection.

3. Click **Connect**.

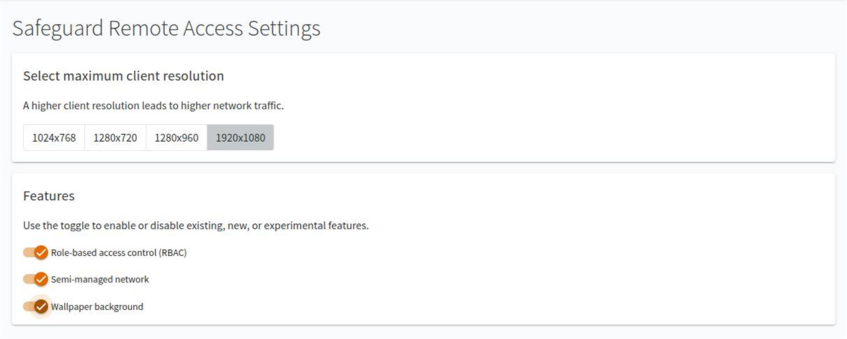
By default, SRA will select a SPS node randomly from the available pool of SPSs in your network. To enable the semi-managed network functionality, go to **Safeguard Remote Access Settings** > **Features** > **Semi-managed network**. If you have only one SPS node configured in your network, then the name of that SPS node in the **Network** field will be grayed out and the dropdown menu will not be available.

Enabling Wallpaper background

With the **Wallpaper background** setting enabled, you can set a custom background for your RDP sessions.

To enable Wallpaper Background

1. Click ⚙ (Settings) and select **Safeguard Remote Access Settings**.
2. Navigate to **Features** > **Wallpaper background**.



Safeguard Remote Access Settings

Select maximum client resolution

A higher client resolution leads to higher network traffic.

1024x768 | 1280x720 | 1280x960 | **1920x1080**

Features

Use the toggle to enable or disable existing, new, or experimental features.

- ✓ Role-based access control (RBAC)
- ✓ Semi-managed network
- ✓ Wallpaper background

3. Enable **Wallpaper background**.

> NOTE: When enabling **Wallpapaer background**, the BG info will also be displayed in all your RDP sessions.

Cloning connections

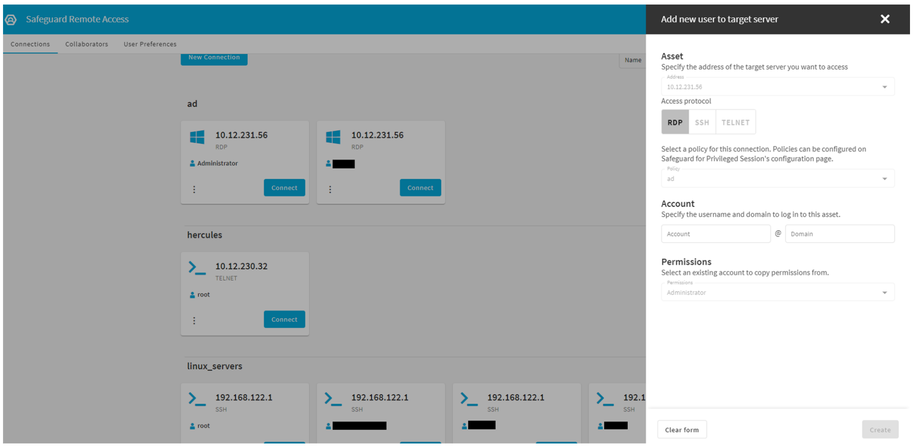
Cloning a connection means that you can connect to a different account with the same permissions.

To clone a connection

1. Go to the **Connections** page and select the connection you would like to clone.
2. Click ⋮ (Options) on the connection card.
3. Select **Clone & Customize**. The **Add new user to target server** side sheet will open.

   Asset, access protocol and policy information are prefilled, as this is an existing connection.
4. Specify the **Account** and **Domain** names for the new connection.
5. In the **Permissions** field, select an existing account to copy permissions from (for example, `root` or `Administrator`).
6. Click **Create**.

Figure 25: Connections > Connection card > ⋮ > Clone & Customize > Permissions — Cloning a connection



Asset

Specify the address of the target server you want to access

Address: 10.12.231.56

Access protocol: [✓ RDP] SSH TELNET

Select a policy for this connection. Policies can be configured on Safeguard for Privileged Session's configuration page.

Policy: ad

Account

Specify the username and domain to log in to this asset.

Account @ Domain

Permissions

Select an existing account to copy permissions from.

Permissions: Administrator

To clone a connection multiple times, use the **Create another** option.

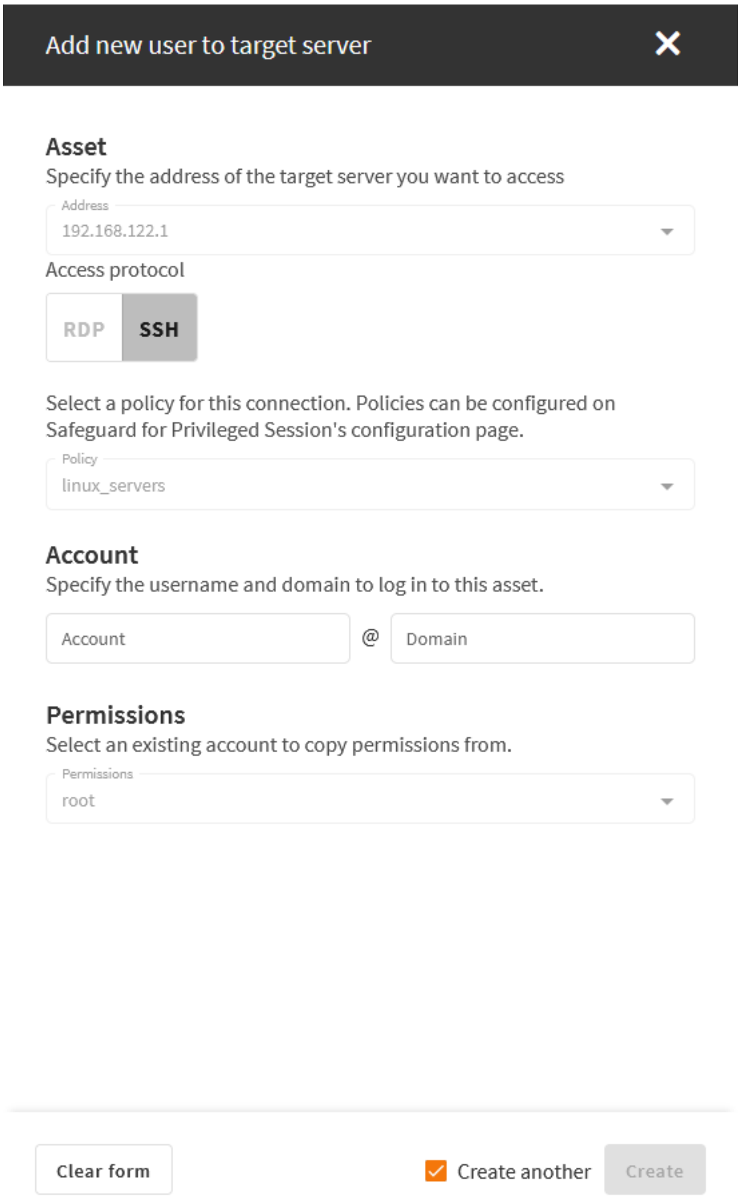
To clone a connection multiple times

1. Follow steps 1-4 of the **To clone a connection** procedure.

   Permissions are cloned from the connection that was last created.

2. Select **Create another**.

Figure 26: Connections > Connection card > ⁝ > Clone & Customize > Add new user to target server > Create another — Cloning a connection multiple times



Add new user to target server ✕

Asset

Specify the address of the target server you want to access

Address: 192.168.122.1

Access protocol

RDP **SSH**

Select a policy for this connection. Policies can be configured on Safeguard for Privileged Session's configuration page.

Policy: linux_servers

Account

Specify the username and domain to log in to this asset.

Account @ Domain

Permissions

Select an existing account to copy permissions from.

Permissions: root

Clear form ☑ Create another Create

3. Click **Create**.

Expected result: The connections that you have created are listed on the **Connections** page.

As long as **Create another** is selected, the side sheet will remain visible and you can create as many clones of the connection as you require, by clicking **Create** repeatedly.

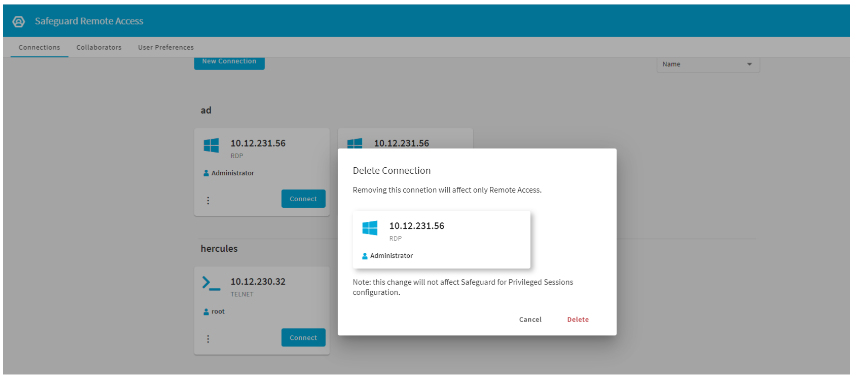
Deleting a connection

When you no longer want to access a connection, delete it from One Identity Safeguard Remote Access (SRA).

To delete a connection

1. Navigate to the **Connections** page and select the connection you want to delete.
2. Click ⋮ (Options) on the connection card.
3. Select **Delete**.

Figure 27: Connections > ⋮ > Delete — Deleting a connection



Delete Connection

Removing this connetion will affect only Remote Access.

Note: this change will not affect Safeguard for Privileged Sessions configuration.

4. Click **Delete**.

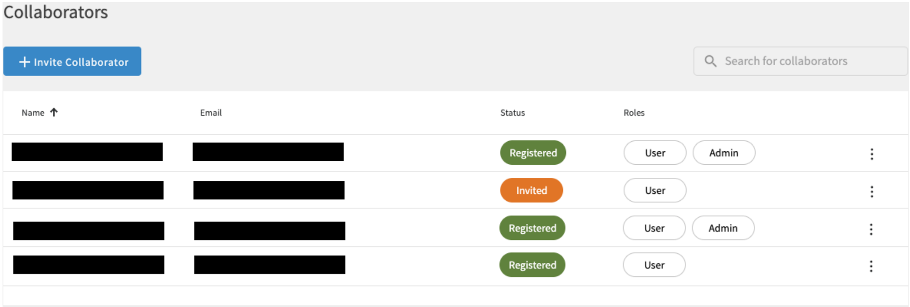
Inviting a collaborator

Inviting a collaborator makes it possible for multiple contributors to have access to One Identity Safeguard Remote Access (SRA).

> NOTE: There are three ways of inviting a collaborator:
>
> - Inviting a collaborator who already has a One Identity Starling account.
> - Inviting and registering an external contributor who does not have a One Identity Starling account.
> - Adding Azure Active Directory users directly.
>
> When you invite One Identity Starling collaborators, you cannot limit the accessibility to connections in SRA. The role-based access control functionality of SRA is available when Azure AD groups are added directly to connections.

On the **Collaborators** page, you can view the list of all collaborators invited or registered to the project, along with their **Name**, **Email**, **Status**, and **Roles**.

Figure 28: Collaborators - Collaborators list



Collaborators

Name ↑	Email	Status	Roles	
[redacted]	[redacted]	Registered	User Admin	⋮
[redacted]	[redacted]	Invited	User	⋮
[redacted]	[redacted]	Registered	User Admin	⋮
[redacted]	[redacted]	Registered	User	⋮

Collaborator statuses and roles

Once invited, collaborators can have two statuses on the **Collaborators** page:

- **Invited**: The collaborator has been invited to your organization, but has not yet confirmed on their side.

  > NOTE: One Identity Starling automatically detects if the invited collaborator does not have an account yet. In this case, the collaborator receives an email with a link to complete the registration process.

  > NOTE: You can cancel and resend invitations in this status, but not in **Registered** status.

- **Registered**: The collaborator has confirmed your invitation on their side.

Collaborators with One Identity Starling accounts can have two distinct roles:

- **Admin**: Collaborators with this role have access to the **Options** page and can configure role-based access control (RBAC). Collaborators with **Admin** role can invite other collaborators and assign roles to other users, set feature flags, and select maximum client resolution under **Safeguard Remote Access Settings**.
- **User**: Collaborators with this role have read-only access to all connections on the **Connections** page, but no configuration rights.

> NOTE: You can change your collaborators' roles by promoting or demoting them.

Searching for collaborators in your organization

If you have a large number of collaborators, you can use the **Search for collaborators** option to narrow down your collaborators list.

If there are no collaborators that match your search (that is, the collaborator is not a member of your SRA service yet), click the **Invite a collaborator** navigation link.

> NOTE: Clicking the **Invite a collaborator** navigation link has the same effect as clicking the **Invite Collaborator** button on the **Collaborators** page.

Inviting an SRA Collaborator to your organization

There are two ways you can invite an SRA collaborator to your organization:

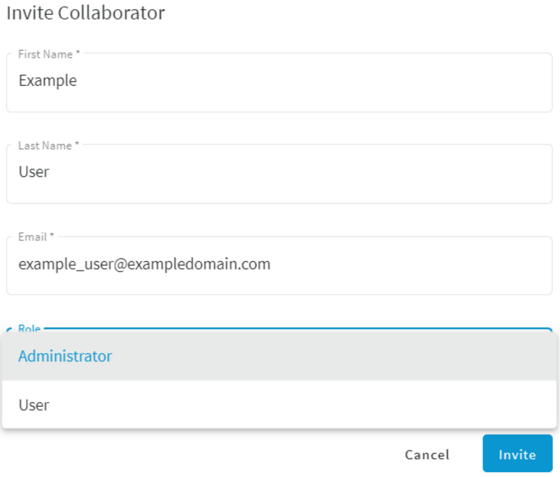
- When there are no matches for your search, using the Invite a collaborator navigation link.
- From the **Collaborators** page.

To invite an SRA collaborator from the Collaborators page

1. Navigate to the **Collaborators** page.
2. Click **Invite Collaborator**.

   A pop-up window appears.

   Figure 29: Collaborators - Inviting a collaborator

   Invite Collaborator

   First Name *: Example

   Last Name *: User

   Email *: example_user@exampledomain.com

   Role: Administrator / User

   Enter the **First Name**, **Last Name**, and **Email** address of the collaborator you want to invite to your organization, then under **Role**, select **Administrator** or **User**.
3. Click **Invite**.

   On the **Collaborators** page, the collaborator you invited appears, with an **Invited** status.

   > TIP: To cancel or re-send your invitation, click ⋮ (Options) next to the collaborator with an **Invited** status, then select **Cancel Invitation** or **Re-send Invitation**.

   Once the collaborator accepts your invitation and confirms on their side, their status changes to **Registered**.

Promoting and demoting collaborators

If you want to change your collaborators' roles, you can promote or demote them.

To promote a collaborator from User to SRA Admin

1. From your collaborators list, select the collaborator you want to promote.
2. Click ⋮ (Options) and select **Remove Collaborator**.

> NOTE: This action will remove the collaborator only from SRA, but not from One Identity Starling.

3. Navigate to the SRA **Collaborators** page.
4. Re-invite the collaborator with **Admin** role.

To a collabdemoteorator from SRA Admin to User

1. From your collaborators list, select the collaborator you want to demote.
2. Click ⋮ (Options) and select **Remove Collaborator**.

   > NOTE: This action will remove the collaborator only from SRA, but not from One Identity Starling.

3. Navigate to the SRA **Collaborators** page.
4. Re-invite the collaborator with **User** role.

> NOTE: You can promote or demote a contributor in One Identity Starling **Services** > **Organization** > **Manage Organization Admins** > ⋮ > **Demote to Collaborator** directly. However, this will not affect the contributor's role in SRA. The only way to switch roles for contributors in SRA is to delete, then re-invite them with a different role.

Restoring a deleted Administrator (or root) connection tile

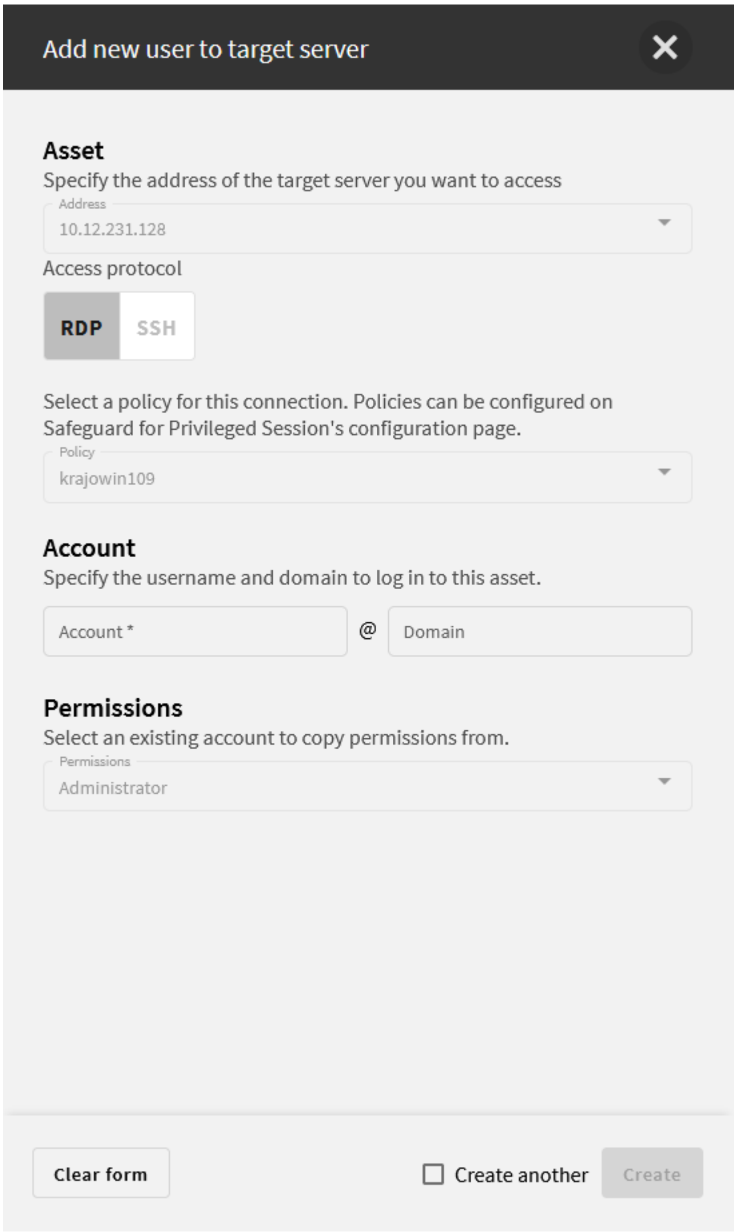
By default, when a connection policy is created in SPS for RDP and/or SSH connections, an **Administrator** (or **root**) connection tile appears for that connection policy on the SRA **Connections** page. If this connection tile was deleted by mistake, there are two ways of restoring it:

(Option 1) Clone a connection from one of your active connections

To restore the Administrator (or root) connection tile by cloning a connection

1. Find the group from which you have deleted the **Administrator** (or **root**) connection tile.
2. Select a connection tile from that group and from ⋮ (Options), choose **Clone & Customize**.
3. Find the **Account** section on **Add new user to target server** and type `Administrator` or `root` into the Account field.

Figure 30: Connections > ⋮ > Clone & Customize > Add new user to target server — Restoring a deleted Administrator (or root) connection tile



Add new user to target server ✕

Asset

Specify the address of the target server you want to access

Address: 10.12.231.128

Access protocol

RDP | SSH

Select a policy for this connection. Policies can be configured on Safeguard for Privileged Session's configuration page.

Policy: krajowin109

Account

Specify the username and domain to log in to this asset.

Account * @ Domain

Permissions

Select an existing account to copy permissions from.

Permissions: Administrator

Clear form   □ Create another   Create

Note, that specifying a domain name is optional.

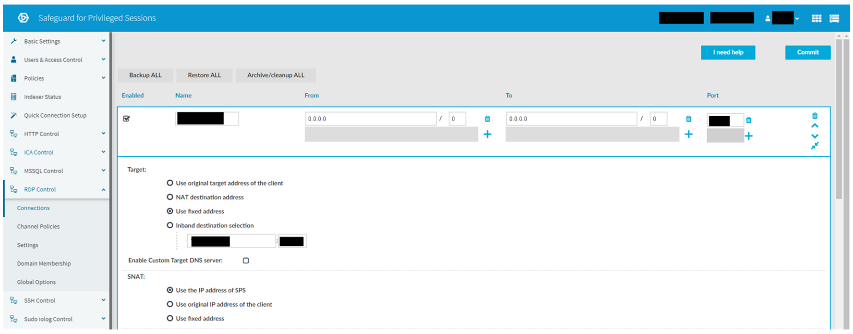
4. Click **Create**.

(Option 2) Create a new connection policy in SPS

To restore the Administrator (or root) connection tile by creating a new connection policy in SPS

1. Open the SPS web interface.
2. Go to **RDP Control** > **Connections** (or **SSH Control** > **Connections** - depending on the type of protocol) and find the connection policy your Administrator (or root) user previously belonged to.
3. Create a new connection policy by copying the details of that previous connection.

Figure 31: RDP control > Connections — Creating a new connection policy for Administrator or root in SPS



Enabled	Name	From	To	Port
☑	[redacted]	0.0.0.0 / 0	0.0.0.0 / 0	[redacted]

Target:

○ Use original target address of the client

○ NAT destination address

● Use fixed address

○ Inband destination selection

[redacted] : [redacted]

Enable Custom Target DNS server: □

SNAT:

● Use the IP address of SPS

○ Use original IP address of the client

○ Use fixed address

4. Commit your changes.
5. Return to SRA and refresh the page. The newly created Administrator (or root) connection tile should be visible.

User-side use cases

This section covers the user-side use cases for One Identity Safeguard Remote Access (SRA).

User web interface location

The web interface for One Identity Safeguard Remote Access is accessible on the link: remote-access.cloud.oneidentity.com.

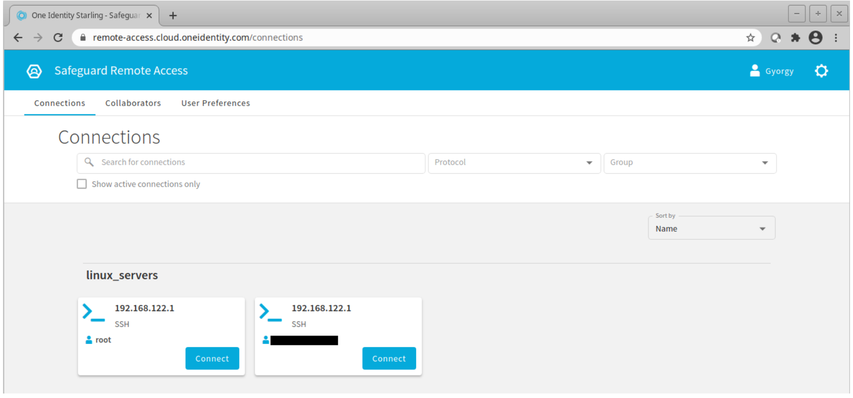
The contents of the interface are loaded from the One Identity Safeguard Remote Access (SRA) subscription where the user is an **Administrator** or **User**. If the user is member of multiple subscriptions, then the appropriate subscription can be selected in the upper right corner.

Connecting to the target server

To connect to the target server

1. Navigate to the **Connections** tab.
2. Use the **Search for connections** field to search for a connection. Alternatively, use the **Protocol** and **Group** fields to narrow down your search options.
3. Select the connection you want to use and click **Connect**.

Figure 32: Connecting to the target server



> NOTE: Different users may see different sets of available connections. The availability of the listed connections depends on the Azure Active Directory (AAD) group membership of the user.

4. When the connection is established to the target server, a new window will open in your browser.

Session window

Once the connection to the target server has been established, your session window will open. In the browser header of Chrome, the user name, server name and domain name for that specific session will be visible.

A pop-up window may prompt you to provide your server-side credentials.

On the left hand side of the session window, you will see a minimized control panel with a >:

Click > once to display the icons-only view of the control panel, and click twice to display the full view.

- > (Minimize control panel)

  Open up or minimize the control panel on the left side.

- ⧉(Copy to clipboard)
- 📋(Paste)
- ⤢ (Enter fullscreen mode)

  > TIP: To exit fullscreen mode, press **Esc**.

- ✕ (End session)

  To disconnect from the target server, click ✕ . Alternatively, clicking ⓐ (One Identity Safeguard Remote Access) in the upper left corner will also disconnect the session.

  > NOTE: Disconnecting from the session does not automatically take you back to the **Connections** page.

Copy-pasting text in an active remote session

When it comes to copy-pasting text with keyboard shortcuts, difficulties may arise from differences between possible shortcuts on the given computer.

Possible keyword shortcuts for copy-pasting:

Windows	Linux	Apple
Ctrl+C	Ctrl+C	Ctrl+Shift+C
Ctrl+V	Ctrl+V	Ctrl+Shift+V

Windows	Linux	Apple
Ctrl+Shift+C	Ctrl+Shift+C	
Ctrl+Shift+V	Ctrl+Shift+V	

> NOTE: For Apple users, copy-pasting text in an active remote session with **Cmd+C** and **Cmd+V** keyboard shortcuts does not work.

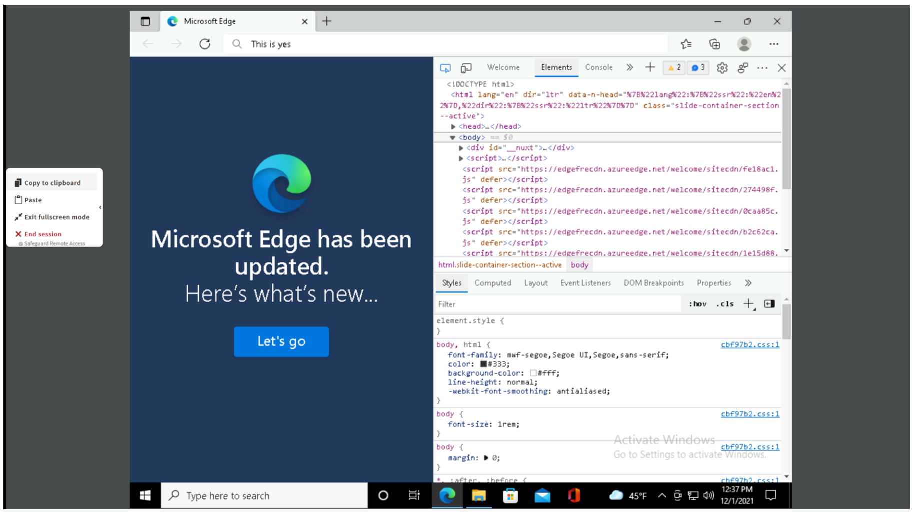
> NOTE: The copy-paste functionality works only for text. The length of the copied text is limited to `32,757` characters for SSH session, and `6,144` characters for RDP session.

Use the copy-paste functionality of the control panel to copy-paste text to and from an active remote session.

To copy-paste text in an active remote session

1. Click › to display the control panel.
2. Select the text you want to copy, and click ⧉ (Copy to clipboard).
3. Insert the copied text into the browser of the remote server.
4. Click 📋 (Paste).

Figure 33: Using Copy to clipboard



Microsoft Edge has been updated.
Here's what's new...

```
<!DOCTYPE html>
 <html lang="en" dir="ltr" data-n-head="%7B%22lang%22:%7B%22ssr%22:%22en%22%7D,%22dir%22:%7B%22ssr%22:%22ltr%22%7D%7D" class="slide-container-section--active">
  ▶ <head>…</head>
  ▼ <body> == $0
    ▶ <div id="__nuxt">…</div>
    ▶ <script>…</script>
     <script src="https://edgefrecdn.azureedge.net/welcome/sitecdn/fe18ac1.js" defer></script>
     <script src="https://edgefrecdn.azureedge.net/welcome/sitecdn/274498f.js" defer></script>
     <script src="https://edgefrecdn.azureedge.net/welcome/sitecdn/0caa85c.js" defer></script>
     <script src="https://edgefrecdn.azureedge.net/welcome/sitecdn/b2c62ca.js" defer></script>
     <script src="https://edgefrecdn.azureedge.net/welcome/sitecdn/1e15d88.
html.slide-container-section--active  body
```

```
element.style {
}
body, html {                                          cbf97b2.css:1
  font-family: mwf-segoe,Segoe UI,Segoe,sans-serif;
  color: ■#333;
  background-color: □#fff;
  line-height: normal;
  -webkit-font-smoothing: antialiased;
}
body {                                                cbf97b2.css:1
  font-size: 1rem;
}
body {                                                cbf97b2.css:1
  margin: ▶ 0;
}
*, :after, :before {                                  cbf97b2.css:1
```

Managing sessions on touch devices

One Identity Safeguard Remote Access (SRA) supports the management of remote sessions in most mobile browsers via touch devices, for example iPad or iPhone. Users can configure connections and open new session windows by touch or by using a stylus.

For the mobile version, the page login works without using any special URI.

> NOTE: On the first visit to the webpage as a SRA Administrator, if the URL does not directly lead to a session window, you will be redirected to the SRA **Settings** page.

To open a new sessions window, select a connection card and touch **Connect**. On the session tab, the screen is automatically fitted to the window size.

You can select the resolution of the stream in **User Preferences**. The default resolution is `1024x768`.

The control panel of the session window is similar to the desktop version with two notable differences:

- To display the built-in on-screen keyboard, click the keyboard icon (⌨). To enter information in the target device's input field, engage the keyboard manually.
- You cannot enter fullscreen mode with the ⤢ (Enter fullscreen mode) button of the control panel if you opened the session on a touch device.

The use of filters on smaller screens is highly recommended, because finding the targeted connection card may take extensive scrolling.

> NOTE: Touch device support was only tested using the Safari browser on iPad and iPhone.

Next generation SSH client

In One Identity Safeguard Remote Access (SRA), the next generation SSH client configuration was developed with a set of functionalities in mind to improve user experience:

- Adaptive applications providing a seamless visual experience between applications (for example, Midnight Commander, a visual file manager that adapts the font size, theme, and resolution of the SSH client automatically).
- Native clipboard support for copy-paste operations.
- Adaptive resolution (that is, when you are resizing the terminal window, the displayed event information adapts to the changed size).
- Screen-reader support for people with visual impairment to help access information on computer screens.
- Web links highlighting.

SSH client functionalities

Once the connection to the target server has been established, your session window opens. A popup window may prompt you to provide your server-side credentials.

In the header of the session window, you will see a control panel with the ⤢ (Enter fullscreen mode) icon.

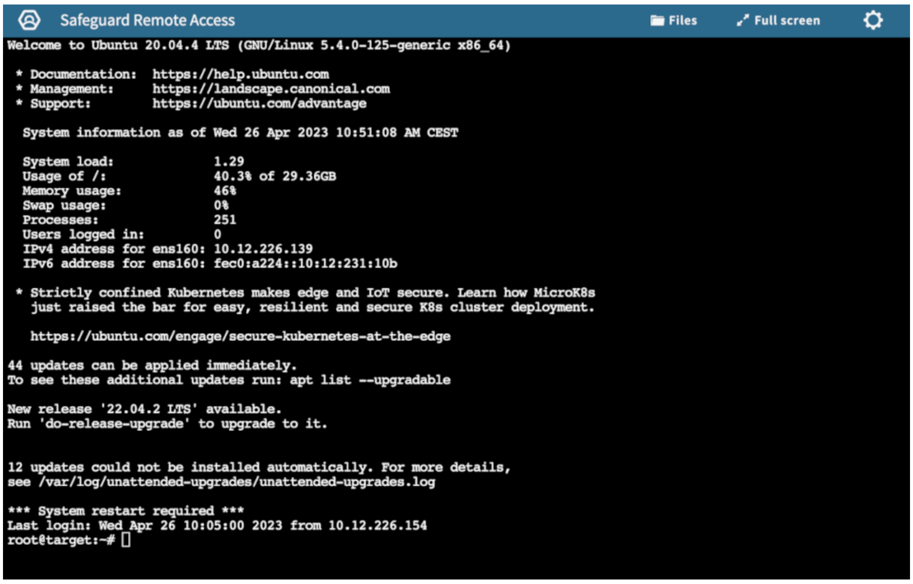
> TIP: To exit fullscreen mode, press **Esc**.

To end a session, you can:

- Close the session window.
- Press **Ctrl+D**.
- Type **`exit`** in the terminal window.

> NOTE: Disconnecting from the session does not automatically take you back to the **Connections** page.

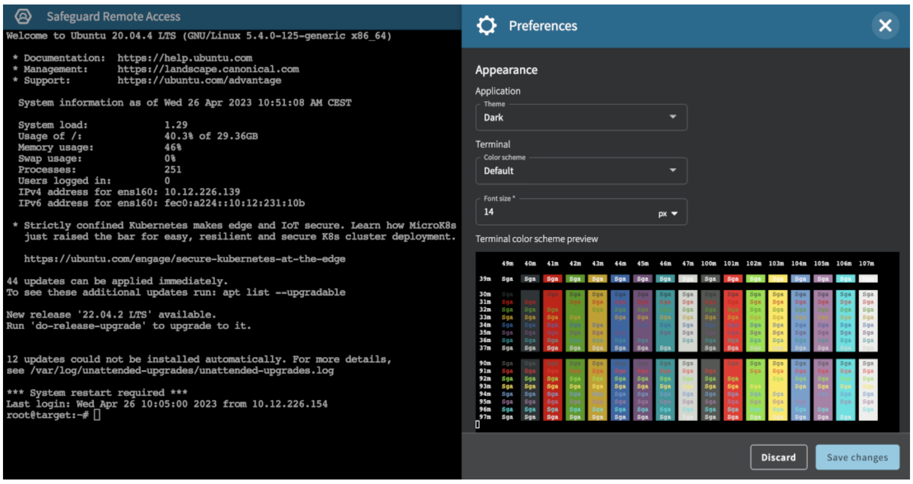
Figure 34: Session view with the next generation SSH client



```
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-125-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 26 Apr 2023 10:51:08 AM CEST

  System load:             1.29
  Usage of /:              40.3% of 29.36GB
  Memory usage:            46%
  Swap usage:              0%
  Processes:               251
  Users logged in:         0
  IPv4 address for ens160: 10.12.226.139
  IPv6 address for ens160: fec0:a224::10:12:231:10b

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

44 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


12 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Wed Apr 26 10:05:00 2023 from 10.12.226.154
root@target:~# 
```

> TIP: You can customize the appearance of your session window by clicking ⚙, setting your **Preferences**, then clicking **Save changes** to save and apply your changes. While you change your settings, the end result is visible in the preview window dynamically.
>
> Under **Preferences**, you can:
>
> - Choose from various pre-set themes for your application.
> - Set the color scheme for your terminal.
> - Change the font to a size that is more preferable to you.

Figure 35: Configuring your display preferences



```
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-125-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 26 Apr 2023 10:51:08 AM CEST

  System load:             1.29
  Usage of /:              40.3% of 29.36GB
  Memory usage:            46%
  Swap usage:              0%
  Processes:               251
  Users logged in:         0
  IPv4 address for ens160: 10.12.226.139
  IPv6 address for ens160: fec0:a224::10:12:231:10b

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

44 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


12 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Wed Apr 26 10:05:00 2023 from 10.12.226.154
root@target:~# 
```

Theme: Dark

Color scheme: Default

Font size *: 14 px

Transferring files in active remote sessions

This section describes how to download and upload files in active remote sessions.

To download files in an active remote session,

1. Navigate to the SRA **Connections** page and find the connection tile you want to work with.
2. In the top-right corner of the session window, select **Files** from the menu bar.

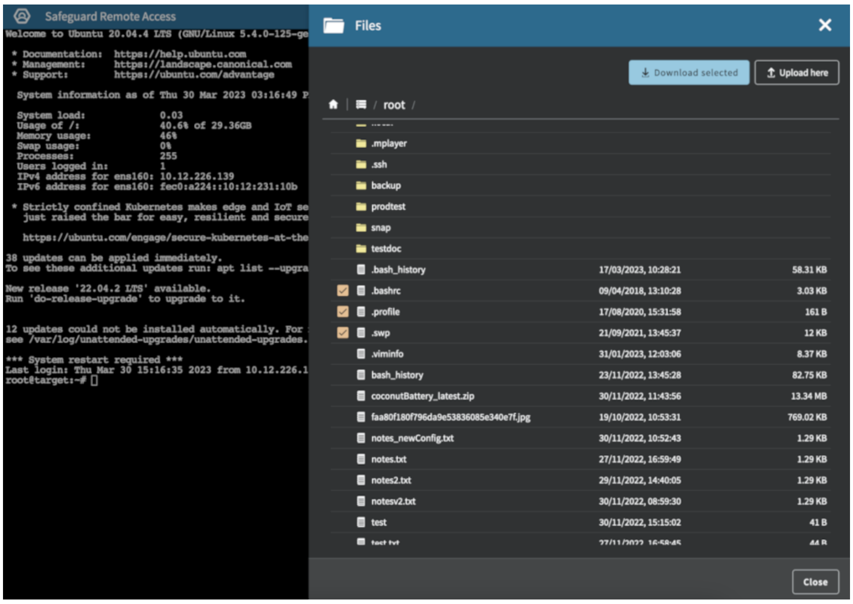
   Above the file tree, there is a folder path to facilitate navigation. By default, you are directed to your **Home** folder.
3. In the file tree, navigate to the file(s) you want to download. You can select the file(s) you want to download by clicking on the filename(s) or the checkbox(es) next to the filename(s).

   When you have selected the file(s) you want to download, click **Download selected**.

   > NOTE: If you want to download multiple files located in different folders, select and add the files to the download queue before moving to a different folder. Otherwise, the files that you have previously selected will not be downloaded.

   If you do not have permission to view a folder, a **Permission denied for selected folder** message will notify you.

Figure 36: SSH session > Files — Downloading files from a remote client



```
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-125-ge

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 30 Mar 2023 03:16:49 P

  System load:             0.03
  Usage of /:              40.6% of 29.36GB
  Memory usage:            46%
  Swap usage:              0%
  Processes:               255
  Users logged in:         1
  IPv4 address for ens160: 10.12.226.139
  IPv6 address for ens160: fec0:a224::10:12:231:10b

 * Strictly confined Kubernetes makes edge and IoT se
   just raised the bar for easy, resilient and secure

   https://ubuntu.com/engage/secure-kubernetes-at-the

38 updates can be applied immediately.
To see these additional updates run: apt list --upgra

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


12 updates could not be installed automatically. For
see /var/log/unattended-upgrades/unattended-upgrades.

*** System restart required ***
Last login: Thu Mar 30 15:16:35 2023 from 10.12.226.1
root@target:~# 
```

	.mplayer		
	.ssh		
	backup		
	prodtest		
	snap		
	testdoc		
	.bash_history	17/03/2023, 10:28:21	58.31 KB
☑	.bashrc	09/04/2018, 13:10:28	3.03 KB
☑	.profile	17/08/2020, 15:31:58	161 B
☑	.swp	21/09/2021, 13:45:37	12 KB
	.viminfo	31/01/2023, 12:03:06	8.37 KB
	bash_history	23/11/2022, 13:45:28	82.75 KB
	coconutBattery_latest.zip	30/11/2022, 11:43:56	13.34 MB
	faa80f180f796da9e53836085e340e7f.jpg	19/10/2022, 10:53:31	769.02 KB
	notes_newConfig.txt	30/11/2022, 10:52:43	1.29 KB
	notes.txt	27/11/2022, 16:59:49	1.29 KB
	notes2.txt	29/11/2022, 14:40:05	1.29 KB
	notesv2.txt	30/11/2022, 08:59:30	1.29 KB
	test	30/11/2022, 15:15:02	41 B
	test.txt	27/11/2022, 16:58:45	44 B

4. (Optional) If you want your files to download in the background while you keep working, check **Start file transfers in the background** above the file tree.
5. Check the downloaded files in your target folder.

   > NOTE: To stop a file from being downloaded, select one of the following two ways:
   >
   > - Open the **Downloads** queue to select the file you do not want to download, and click **X**.
   > - If you are using Google Chrome as a browser (recommended), navigate to the downloaded files lane at the bottom of the page to select the file you do not want to download, and click **Cancel**. You can also **Pause** and **Resume** downloads. This feature is applicable only to Google Chrome.

To upload files in an active remote session,

1. Navigate to the SRA **Connections** page and find the connection tile you want to work with.
2. In the top-right corner of the session window, select **Files** from the menu bar.

   Above the file tree, there is a folder path for easy navigation. By default, you are directed to your **Home** folder.
3. Upload your file(s) by either of these methods:
   - Click **Upload here** and find the file(s) on your computer that you want to upload.
   - Drag and drop files from your computer to upload them.

   > TIP: The number of files being uploaded is visible in the **Uploads(<number-of-downloads>)** counter. If a version of the file already exists on the remote client, you can decide whether you want to override the file or change the file name to

keep the previous file version as well. The folder you have uploaded your file into is refreshed automatically.

4. (Optional) To have file upload run in the background, check **Start file transfers in the background**.
5. (Optional) To check the progress of the upload, click **Uploads**.
6. Check the uploaded files in your target folder.

You can upload and download files in an active remote session simultaneously. All downloads and uploads can be managed individually within the queue. The **Downloads** | **Uploads** buttons disappear if all files have been processed.

NOTE: During file transfer, the **All files are processed** status can refer to the following scenarios:

- The file is uploaded | downloaded.
- The user started the file transfer, but the server declined the request and the file was deleted from the file transfer queue.
- The user started the file transfer, but decided to cancel it before the upload | download is completed.

NOTE: SRA uses the JEDEC standard for file size calculation, where a kilobyte is considered as 1,024 bytes instead of 1,000 bytes. This could lead to scenarios where you can observe differences between the file sizes of the transferred files (for example, the file size might be 13.34 MB during download and 14 MB after download).

User Preferences tab

Setting the default RDP image resolution

Setting the RDP image resolution according to your system results in a better stream quality.

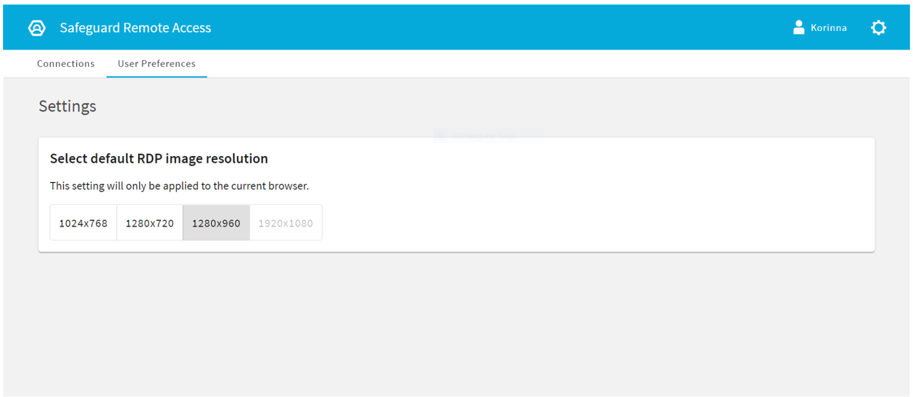
NOTE: Available choices may be limited by the `Administrator`.

To set the default RDP image resolution:

1. Navigate to the **User Preferences** tab.
2. Find the **Set the default resolution**.
3. Select the preferred image resolution.

   NOTE: The default value is `1024x768`. The setting can be applied only to the current browser.

Figure 37: Setting the default RDP image resolution



Settings

Select default RDP image resolution

This setting will only be applied to the current browser.

1024x768 | 1280x720 | 1280x960 | 1920x1080

Appendix

This section covers One Identity Safeguard for Privileged Sessions (SPS) related topics that are necessary for the One Identity Safeguard Remote Access (SRA) configuration to work properly.

Configuring usermapping policies

For SSH, RDP, Telnet, and Citrix ICA connections, usermapping policies can be defined. A usermapping policy describes who can use a specific username to access the remote server: only members of the specified local or LDAP usergroups (for example, `administrators`) can use the specified username (for example, `root`) on the server.

⚠ **CAUTION:**

In SSH connections, the users must use the following as their username: `gu=username@remoteusername`, where `username` is the username used in the LDAP directory, SPS will use this username to determine their group memberships, and `remoteusername` is the username they will use on the remote server. For example, to access the example.com server as root, use:

```
gu=yourldapusername@root@example.com
```

For the username of SSH users, only valid UTF-8 strings are allowed.

⚠ **CAUTION:**

In Telnet connections, usermapping policy works only if Extract username from the traffic is enabled.

When configuring ICA connections, also consider the following:

⚠ **CAUTION:**

If the clients are accessing a remote application or desktop that is shared for Anonymous users (that is, the Users properties of the application is set to `Allow anonymous users` in the Citrix Delivery Services Console), the actual remote session will be running under an Anonymous account name (for example, `Anon001`, `Anon002`, and so on), not under the username used to access the remote server. Therefore, you need to enable usermapping to the `Anon*` usernames.

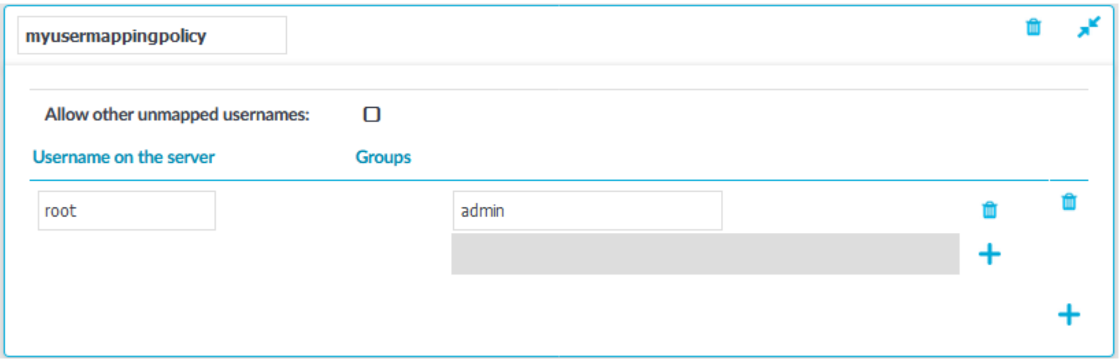
To accomplish this, create a usermapping policy and set the Username on the server option to `Anon*`, and the Groups option to `*`, then use this usermapping policy in your ICA connections.

NOTE: Starting from SPS version 3.2, usermapping is possible only when gateway authentication is used as well.

To configure usermapping

1. Navigate to **Policies** > **Usermapping Policies**.

   Figure 38: Policies > Usermapping Policies — Configuring usermapping policies

   myusermappingpolicy

   Allow other unmapped usernames: □

Username on the server	Groups
root	admin

2. Click + to create a new policy, and enter a name for the policy.

3. Click + and enter the username that can be used to access the remote server (for example `root`) into the **Username on the server** field. SPS will use this username in the server-side connection. To permit any username on the server side, enter an asterisk (*****).

4. Select **Groups**, click + and specify who is permitted to use the remote username set in the **Username on the server** field.

   - If you have an LDAP Server set in the connection policy where you will use usermapping, enter the name of the local or LDAP usergroup (for example **`admins`**) whose members will be permitted to use the remote username.

     > NOTE: The LDAP server configured in the connection policy is not necessarily the same as the LDAP server used to authenticate the users accessing the SPS web interface.

   - If you do not authenticate the connections to an LDAP server, enter the name of the userlist whose members will be permitted to use the remote username.

   Repeat this step to add further groups if needed.

5. Repeat steps 3-4 to add further usernames if needed.

6. To permit other users, who are not explicitly listed in the Usermapping Policy access the remote servers, select the **Allow other unmapped usernames** option. Note that these users must use the same username on the SPS gateway and the remote server.

7. Click **Commit**.

8. Navigate to the **Connections** page of the traffic (for example to **SSH Control** > **Connections**), and select the connection policy to modify.
9. Select the usermapping policy created in Step 2 from the **Usermapping policy** field.
10. Click Commit.

    NOTE: For RDP connections, usermapping is possible only when gateway authentication is used as well. When configuring usermapping for RDP connections, configure gateway authentication.

Configuring local Credential Stores

The following describes how to configure a local Credential Store that stores the credentials used to login to the target host.

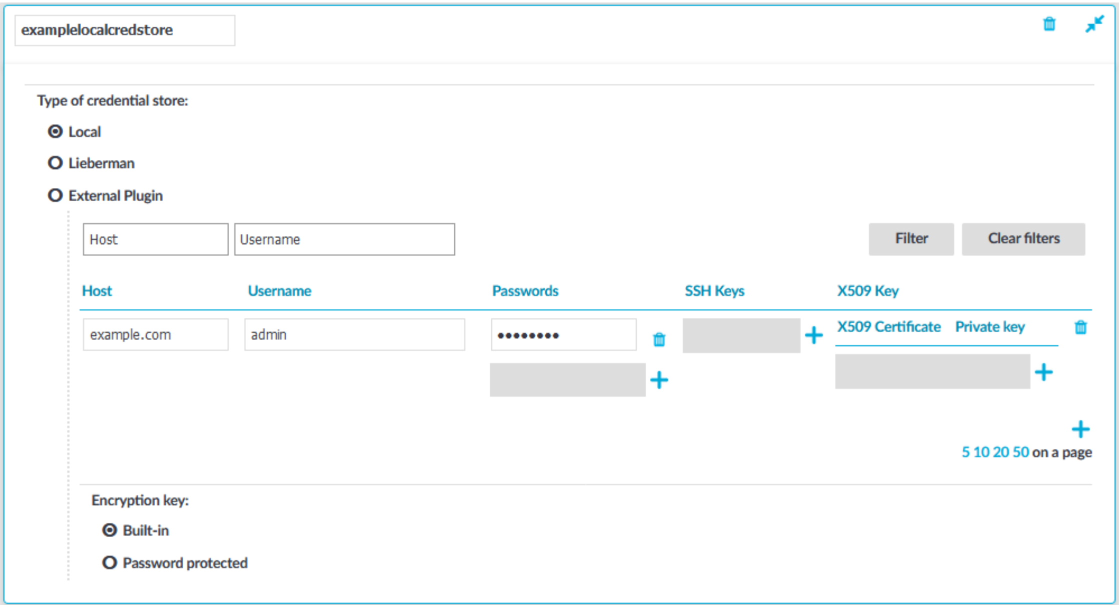
Prerequisites

> NOTE: Users accessing connections that use Credential Stores to authenticate on the target server must authenticate on SPS using gateway authentication or an AA plugin. Therefore gateway authentication or an AA plugin must be configured for these connections.

To configure a local Credential Store that stores the credentials used to login to the target host

1. Navigate to **Policies** > **Credential Stores**.
2. Click + and enter a name for the Credential Store.
3. Select **Local**.
4. Select **Encryption key** > **Built-in**. That way the credentials will be encrypted with a built-in password, and the Credential Store is automatically accessible when SPS boots up.

Figure 39: Policies > Credential Stores > Local — Configuring local Credential Stores



examplelocalcredstore

Type of credential store:

● Local

○ Lieberman

○ External Plugin

Host	Username	Passwords	SSH Keys	X509 Key
example.com	admin	••••••••		X509 Certificate / Private key

Encryption key:

● Built-in

○ Password protected

5. Add credentials to the Credential Store.

   a. Click + and enter the destination host and the username. For the destination host, you can use hostname, IP address, or subnet as well. To use the same credentials for every destination host, enter the `0.0.0.0/0` subnet. To use the credentials only on the hosts of a specific domain, enter `*.domain`. Note that:

      - Usernames are case sensitive.

      - To authenticate users of a Windows domain, enter the name of the domain into the **Host** field.

      Use an IPv4 address.

   b. Set the credentials. SPS will use these credentials to login to the destination host if the credential store is selected in a Connection policy. If more than one credential is specified to a host-username pair, SPS will attempt to use the credentials as the destination host requests it.

      - To add a password, click **Passwords >** +, then enter the password corresponding to the username.

      - To upload a private key, click **SSH Keys >** + > ✎, then paste or upload a private key.

        > NOTE: If the private key is protected by a passphrase, enter the passphrase. The passphrase is needed only once during the upload, it

> is not required for the later operation of the Credential Store.

- To generate a keypair on SPS click **SSH Keys >** + **>** ✎ , set the length and type of the key, then click **Generate**. After that, click the fingerprint of the key to download the public part of the keypair. There is no way to download the private key from the SPS web interface.

  > NOTE:
  >
  > > TIP: One Identity recommends using 2048-bit RSA keys (or stronger).

- To upload a certificate and the corresponding private key, click **X509 Keys >** + **>** ✎ , then paste or upload a certificate and the private key.

  > NOTE: If the private key is protected by a passphrase, enter the passphrase. The passphrase is needed only once during the upload, it is not required for the later operation of the Credential Store.

> NOTE: SPS accepts passwords that are not longer than 150 characters and supports the following characters:
>
> - Letters A-Z, a-z
> - Numbers 0-9
> - The space character
> - Special characters: !"#$%&'()*+,-./:;<>=?@[]\^-`{}_|

c. Repeat the previous step to add further credentials to the username as necessary.

6. Repeat the previous step to add further hosts or usernames as necessary.

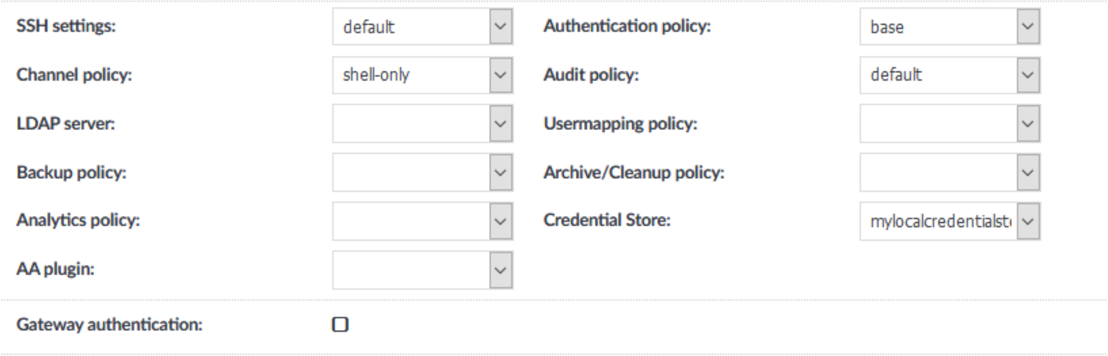
   > NOTE: Credential Stores can be used together with usermapping policies to simplify the administration of users on the target hosts.
   >
   > For more information, see Configuring usermapping policies on page 54.

7. Click Commit.

8. Navigate to the Connection policy where you want to use the Credential Store (for example, to **SSH Contro** > **Connections**), select the Credential Store to use in the **Credential Store** field, then click Commit.

   > NOTE: The Connection Policy will ignore the settings for server-side authentication (set under **Relayed authentication methods**) if a Credential Store is used in the Connection Policy.

Figure 40: <Protocol name> Control > Connections — Select a Credential Store to use



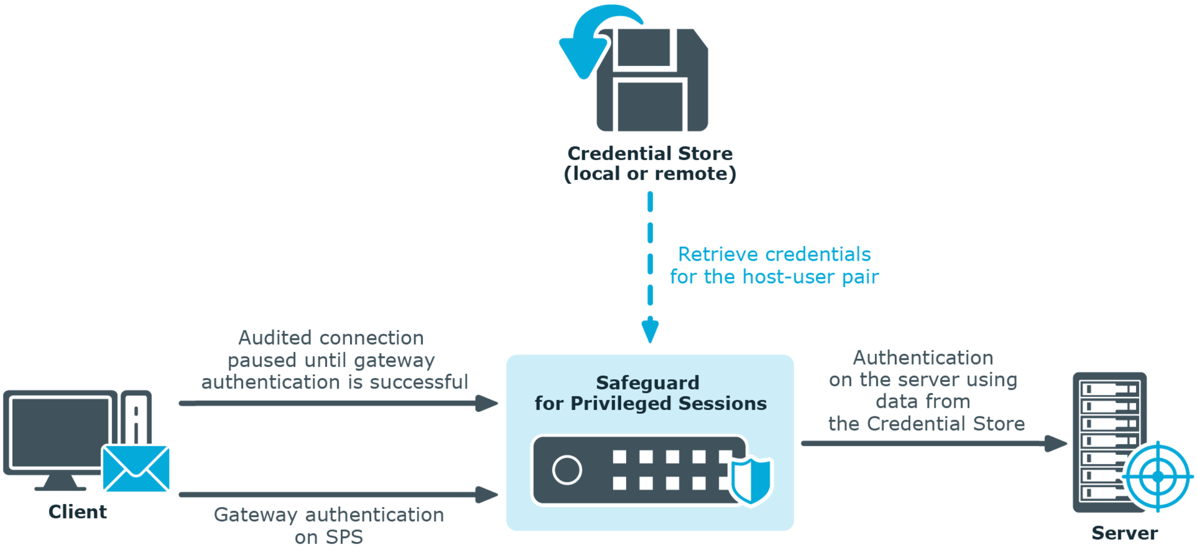
SSH settings:	default	Authentication policy:	base
Channel policy:	shell-only	Audit policy:	default
LDAP server:		Usermapping policy:	
Backup policy:		Archive/Cleanup policy:	
Analytics policy:		Credential Store:	mylocalcredentialst
AA plugin:			
Gateway authentication:	□		

Using credential stores for server-side authentication

Credential Stores offer a way to store user credentials (for example, passwords, private keys, certificates) and use them to log in to the target server, without the user having access to the credentials. That way, the users only have to perform gateway authentication on SPS with their usual password (or to an LDAP database), and if the user is allowed to access the target server, SPS automatically logs in using the Credential Store.

> NOTE: Keyboard-interactive authentication is not supported when using credential stores.

Figure 41: Authenticating using Credential Stores



Credential Stores can be stored locally on SPS, or on a remote device. For remote Credential Stores, SPS integrates with external authentication and authorization systems using plugins.

NOTE: After performing a successful gateway authentication, if the credential store does not contain a password for the user, the user is prompted for the server-side password as a fallback.

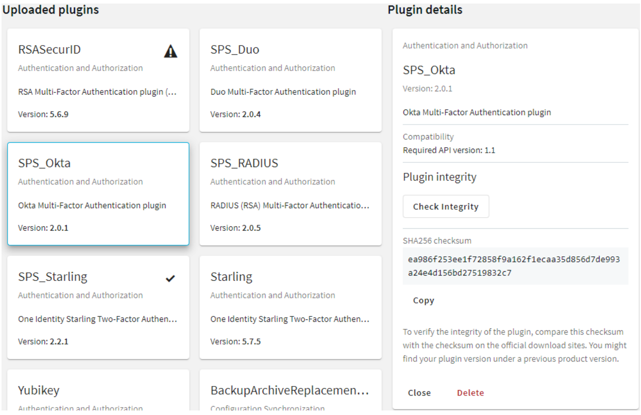
In case of authenticating to RDP servers using Network Level Authentication (NLA), the server-side password is prompted at the start of the connection. If there is no password in the credential store for the user and the server-side password is incorrect, the connection is terminated.

Using plugins

To download the official plugins for your product version, navigate to the product page on the Support Portal. The not officially supported plugins are also available on GitHub .

To write your own custom plugin, feel free to use our Plugin SDK.

Figure 42: Basic Settings > Plugins — Viewing the uploaded plugins



Uploaded plugins

RSASecurID ⚠
Authentication and Authorization
RSA Multi-Factor Authentication plugin (...
Version: 5.6.9

SPS_Duo
Authentication and Authorization
Duo Multi-Factor Authentication plugin
Version: 2.0.4

SPS_Okta
Authentication and Authorization
Okta Multi-Factor Authentication plugin
Version: 2.0.1

SPS_RADIUS
Authentication and Authorization
RADIUS (RSA) Multi-Factor Authenticatio...
Version: 2.0.5

SPS_Starling ✓
Authentication and Authorization
One Identity Starling Two-Factor Authen...
Version: 2.2.1

Starling
Authentication and Authorization
One Identity Starling Two-Factor Authen...
Version: 5.7.5

Yubikey
Authentication and Authorization

BackupArchiveReplacemen...
Configuration Synchronization

Plugin details

Authentication and Authorization
SPS_Okta
Version: 2.0.1
Okta Multi-Factor Authentication plugin

Compatibility
Required API version: 1.1

Plugin integrity
Check Integrity

SHA256 checksum
ea986f253ee1f72858f9a162f1ecaa35d856d7de993
a24e4d156bd27519832c7

Copy

To verify the integrity of the plugin, compare this checksum with the checksum on the official download sites. You might find your plugin version under a previous product version.

Close Delete

The following plugin types can be uploaded to SPS:

- Authentication and Authorization plugins
- Credential Store plugins
- Configuration Synchronization plugins
- Signing CA plugins

Configuring connections

This section describes how to configure connections.

NOTE:

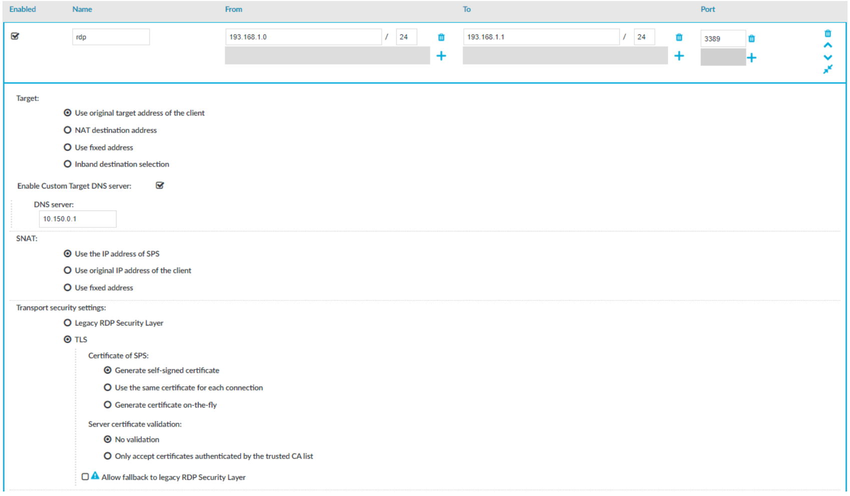
When configuring HTTP or SSH connections, avoid using the IP address configured for administrator or user login on SPS.

To configure connections

1. Select the type of connection from the main menu.
   - To configure an HTTP connection, select **HTTP Control** > **Connections**.
   - To configure an ICA connection, select **ICA Control** > **Connections**.
   - To configure a Remote Desktop connection, select **RDP Control** > **Connections**.
   - To configure a Secure Shell connection, select **SSH Control** > **Connections**.
   - To configure a Telnet connection, select **Telnet Control** > **Connections**.
   - To configure a VNC connection, select **VNC Control** > **Connections**.
2. Click + to define a new connection and enter a name that identifies the connection (for example, `admin_mainserver`).

   > TIP: Use descriptive names that give information about the connection, for example, refer to the name of the accessible server, the allowed clients, and so on.

Figure 43: <Protocol name> Control > Connections — Configuring connections



Enabled	Name	From	To	Port
☑	rdp	193.168.1.0 / 24	193.168.1.1 / 24	3389

Target:

- ● Use original target address of the client
- ○ NAT destination address
- ○ Use fixed address
- ○ Inband destination selection

Enable Custom Target DNS server: ☑

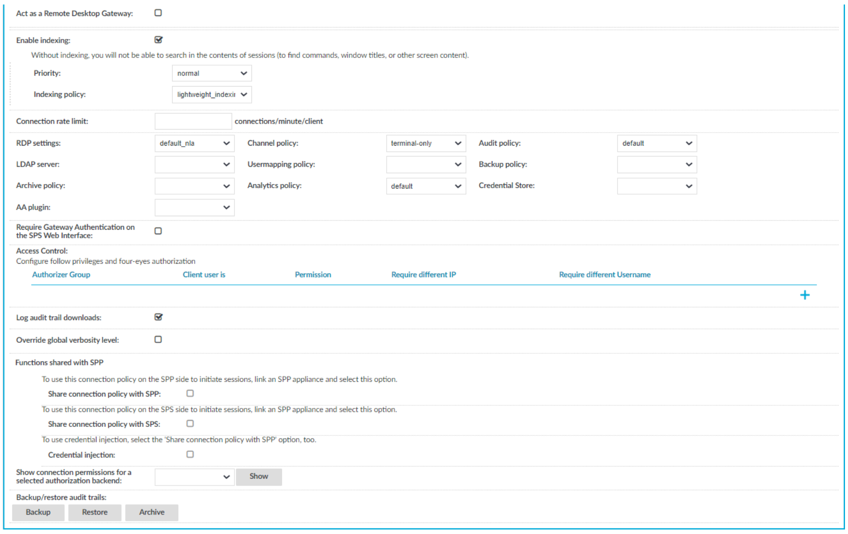
DNS server: 10.150.0.1

SNAT:

- ● Use the IP address of SPS
- ○ Use original IP address of the client
- ○ Use fixed address

Transport security settings:

- ○ Legacy RDP Security Layer
- ● TLS
  - Certificate of SPS:
    - ● Generate self-signed certificate
    - ○ Use the same certificate for each connection
    - ○ Generate certificate on-the-fly
  - Server certificate validation:
    - ● No validation
    - ○ Only accept certificates authenticated by the trusted CA list
  - □ ⚠ Allow fallback to legacy RDP Security Layer



Act as a Remote Desktop Gateway: □

Enable indexing: ☑

Without indexing, you will not be able to search in the contents of sessions (to find commands, window titles, or other screen content).

Priority: normal

Indexing policy: lightweight_indexi

Connection rate limit: connections/minute/client

RDP settings:	default_nla	Channel policy:	terminal-only	Audit policy:	default
LDAP server:		Usermapping policy:		Backup policy:	
Archive policy:		Analytics policy:	default	Credential Store:	
AA plugin:					

Require Gateway Authentication on the SPS Web Interface: □

Access Control:
Configure follow privileges and four-eyes authorization

Authorizer Group	Client user is	Permission	Require different IP	Require different Username

Log audit trail downloads: ☑

Override global verbosity level: □

Functions shared with SPP

To use this connection policy on the SPP side to initiate sessions, link an SPP appliance and select this option.

Share connection policy with SPP: □

To use this connection policy on the SPS side to initiate sessions, link an SPP appliance and select this option.

Share connection policy with SPS: □

To use credential injection, select the 'Share connection policy with SPP' option, too.

Credential injection: □

Show connection permissions for a selected authorization backend:

Backup/restore audit trails:

3. In the **From** field, enter the IP address of the client that is permitted to access the server. To list additional clients, click + .

   You can use an IPv4 or an IPv6 address. To limit the IP range to the specified address, set the prefix to **32** (IPv4) or **128** (IPv6).

   Alternatively, you can enter a hostname instead. SPS automatically resolves the hostname to an IP address.

   > NOTE: Note the following limitations:
   >
   > - To resolve the hostnames, SPS uses the Domain Name Servers set in the **Basic Settings** > **Network** > **Naming** > **Primary DNS server** and **Secondary DNS server** fields.
   > - If the Domain Name Server returns multiple IP addresses, SPS randomly selects from the list.

4. In the **To** field, enter the IP address that the clients request.

   You can use an IPv4 or an IPv6 address. To limit the IP range to the specified address, set the prefix to **32** (IPv4) or **128** (IPv6).

   Alternatively, you can enter a hostname instead. SPS automatically resolves the hostname to an IP address.

   > NOTE: Note the following limitations:
   >
   > - To resolve the hostnames, SPS uses the Domain Name Servers set in the **Basic Settings** > **Network** > **Naming** > **Primary DNS server** and **Secondary DNS server** fields.
   > - If the Domain Name Server returns multiple IP addresses, SPS randomly selects from the list.

   - In non-transparent mode, enter the IP address of an SPS logical interface.
   - In transparent mode, enter the IP address of the protected server.

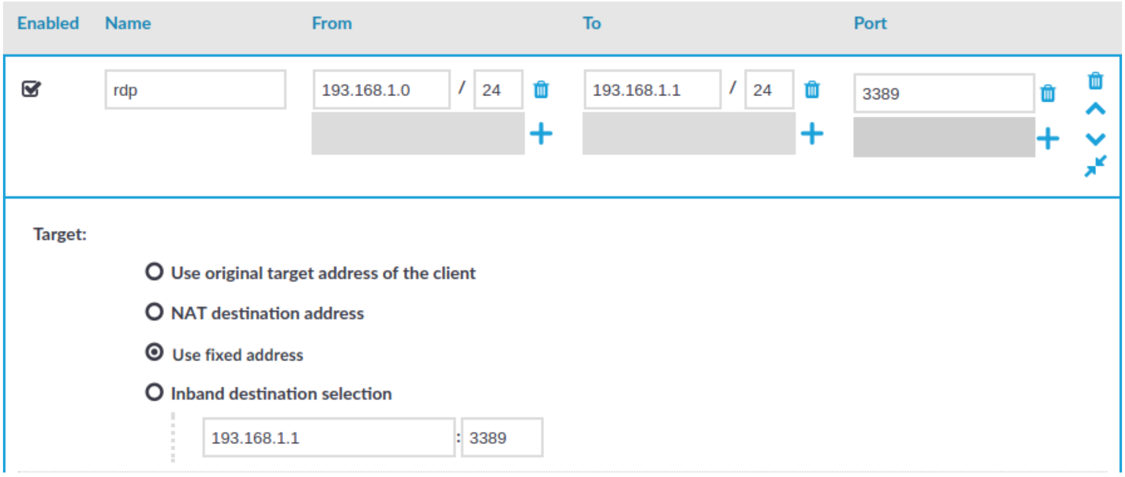
To add additional IP addresses, click + .

5. If the clients use a custom port to address the server instead of the default port of the protocol, in the **Port** field, enter the port number that the clients request. To list additional port numbers, click + .

   > NOTE: SPS can handle a maximum of 15 unique ports per connection policy. If you want to add more than 15 custom ports, create additional connection policies.

6. *Non-transparent mode*: In the **Target** field, enter the IP address and port number of the target server. SPS connects all incoming client-side connections to this server.

Figure 44: <Protocol name> Control > Connections — Configuring non-transparent connections



Enabled	Name	From	To	Port
☑	rdp	193.168.1.0 / 24	193.168.1.1 / 24	3389

Target:

○ Use original target address of the client

○ NAT destination address

● Use fixed address

○ Inband destination selection

193.168.1.1 : 3389

7. If needed, configure advanced settings (for example, network address translation, channel policy, gateway authentication, various policies, or other settings).

8. To save the connection, click **Commit**.

   > TIP: To temporarily disable a connection, deselect the checkbox of the connection.

9. If needed, reorder the list of the connection policies. You can move connection policies by clicking the ⌃ and ⌄ buttons.

   SPS compares the connection policies to the parameters of the connection request one-by-one, starting with the first policy in the policy list. SPS applies to the connection the first connection policy that completely matches the connection request.

10. Depending on your needs and on your environment, you can configure the following settings for your connections:

    - Modify the destination or source addresses of the connections.
    - Select a **Backup Policy** and an **Archiving Policy** for the audit trails and indexes of the connection.

If you have indexed trails, the index is archived every 30 days.

> ⚠ **CAUTION:**
>
> **Hazard of data loss! Make sure you also back up your data besides archiving it.**
>
> **If a system crash occurs, you can lose up to 30 days of index, since the index is only archived every 30 days.**

> NOTE: The backup and archive policies set for the connection apply only to the audit trails and indexes of the connection. General data about the connections that is displayed on the **Search** page is archived and backed up as part of the system-backup process of SPS.

- To timestamp, encrypt, or sign the audit trails, configure an **Audit Policy** to suit your needs.

  > ⚠ **CAUTION:**
  >
  > **In RDP connections, if the client uses the Windows login screen to authenticate on the server, the password of the client is visible in the audit trail. To avoid displaying the password when replaying the audit trail, encrypt the upstream traffic in the audit trail using a separate certificate from the downstream traffic.**

- Require the users to authenticate themselves not only on the target server, but on SPS as well.
- Require four-eyes authorization on the connections, with the possibility of an auditor monitoring the connection in real-time.
- In the case of certain connections and scenarios (for example SSH authentication, gateway authentication, Network Level Authentication (NLA) connections), SPS can authenticate you to an LDAP database, or retrieve your group memberships. To use these features, select an **LDAP Server**.

  > NOTE: To display the usergroups that can access a specific Connection Policy, open the Connection Policy, then on the **Connections** page, select **Show connection permissions** > **Show**.

- To limit the number of new connection requests accepted from a single client IP address per minute, in the **Connection rate limit** field, enter the maximum number of accepted connections.
- If you have joined an SPP appliance to SPS and want to share specific SPS functions with SPP, use the **Functions shared with SPP** option.

  To share an RDP or an SSH connection policy with SPP to initiate sessions, select **Share connection policy with SPP**.

11. If your clients and servers support it, configure the connection to use strong encryption.
12. For graphical connections, adjust the settings of your servers for optimal performance:

- ⚠ **CAUTION:**

  For optimal performance and text recognition in graphical protocols, disable antialiasing on your servers. Antialiased text in the audit trails of RDP, VNC, and X11 connections is not recognized by the OCR engine of the Audit Player. The indexer service recognizes antialiased text, but its accuracy depends on the exact antialiasing settings. To properly index the trails of these connections, disable antialiasing.

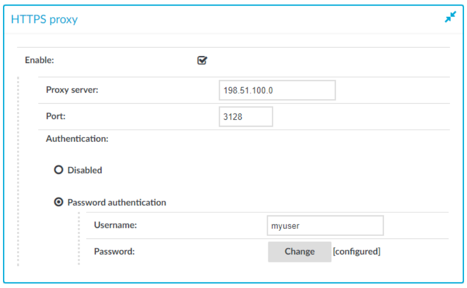
  Note that by default, antialiasing is enabled on Windows Vista and later versions. Antialiasing is also called font smoothing. To optimize performance, disable ClearType, which is an antialiasing technology used on Microsoft Windows.

- When processing RDP connections, SPS attempts to extract the username from the connection.

HTTPS proxy

The **HTTPS proxy** settings must be configured if your company policies do not allow devices to connect directly to the web. Once configured, SPS uses the configured proxy server for outbound web requests to external integrated services, such as Join to Starling or SPS plugins.

Figure 45: Basic Settings > Network > HTTPS proxy



HTTPS proxy

Enable: ☑

Proxy server: 198.51.100.0

Port: 3128

Authentication:

○ Disabled

● Password authentication

Username: myuser

Password: Change [configured]

- **Proxy server**: The IP address or DNS name of the proxy server.
- **Port**: The IP address or DNS name of the proxy server.

  NOTE:

  If different ports are specified in the **Proxy server** and the **Port** field, the **Port** field takes precedence.

- **Username**: The user name used to connect to the proxy server.

> NOTE:
>
> The username and password are only required if your proxy server requires them to be specified.

- **Password**: The password required to connect to the proxy server.

  > NOTE:
  >
  > The username and password are only required if your proxy server requires them to be specified.

Joining SPS to One Identity Starling

This section describes how to use SPS with One Identity Starling and how to take advantage of companion features from Starling products, such as Two-Factor Authentication (2FA) and Identity Analytics.

Prerequisites

- An existing Starling organization (tenant).

  > NOTE: Consider the following:
  >
  > - If you have several Starling organizations, you can join your SPS to any of the existing organizations. However, ensure that you remember the Starling organization you joined to your SPS. This might be required if there is a join failure and you need to unjoin SPS from the respective Starling organization.
  > - To use Starling with SPS, you need a Starling organization and account within a United States or a European Union data center. Note that if you want to use Starling 2FA, you must use a United States data center (European Union data center is not yet supported).

To join SPS to One Identity Starling

1. Navigate to **Basic Settings** > **Starling Integration**.

   > ⚠ **CAUTION: If SPS nodes are joined to a cluster, ensure that you initiate your Starling integration from the Central Management node.**

2. To check the availability of SPS and Starling, that is, if SPS can connect directly to the web and SPS can access Starling, click **Check availability**.

   - If your SPS cannot connect directly to the web, check your Internet connection and ensure that SPS can connect to the web, then re-initiate the process of joining your SPS to Starling. Ensure that SPS can access the following websites:

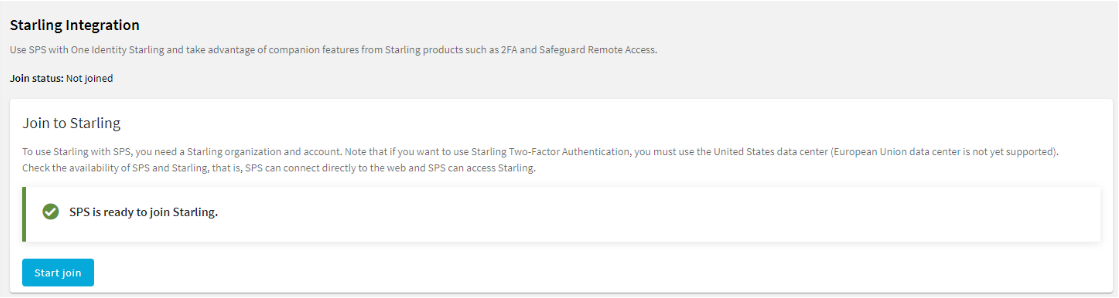
    - account.cloud.oneidentity.com
    - sts.cloud.oneidentity.com
    - accountsupervisor.cloud.oneidentity.com
    - oneidentitycloud.statuspage.io

  If your SPS is behind a web proxy, navigate to **Basic Settings** > **Network** > **HTTPS Proxy** and configure the proxy settings.

  > NOTE: Currently, only built-in Certificate Authorities are supported. If the web proxy replaces the certificates of the Starling website on-the-fly, the join process might fail.

- If SPS cannot access Starling, wait until Starling is available and re-initiate the process of joining your SPS to Starling.

Figure 46: Basic Settings > Starling Integration — SPS is ready to join Starling



Starling Integration

Use SPS with One Identity Starling and take advantage of companion features from Starling products such as 2FA and Safeguard Remote Access.

Join status: Not joined

Join to Starling

To use Starling with SPS, you need a Starling organization and account. Note that if you want to use Starling Two-Factor Authentication, you must use the United States data center (European Union data center is not yet supported). Check the availability of SPS and Starling, that is, SPS can connect directly to the web and SPS can access Starling.

✓ SPS is ready to join Starling.

3. When SPS is ready to join Starling, click **Start join**.

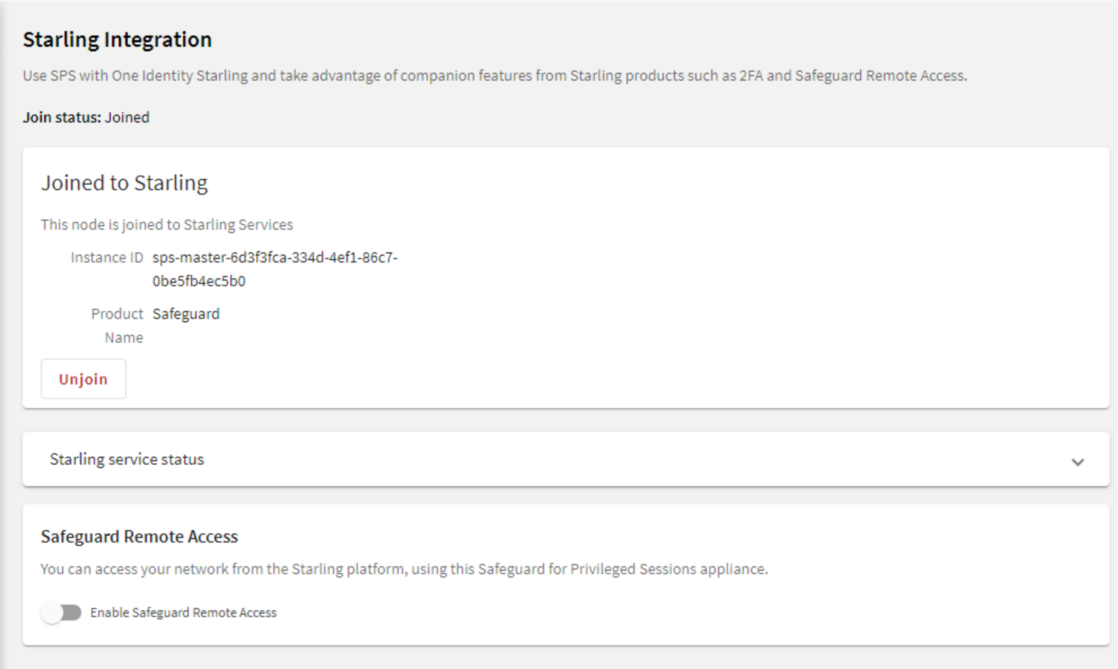
   The One Identity Starling site will open on a new tab.

   > NOTE: Once you click **Start join**, you cannot stop the process and your SPS machine will be joined to Starling. Ensure that you continue with the join process, and once the join process is complete, if required, you can unjoin SPS from Starling.

4. To allow SPS to access your Starling organization and the services that you have subscribed to, click **Allow**.

   The **Join to Starling** screen is displayed.

Figure 47: Basic Settings > Starling Integration — Example of SPS joined to Starling



Starling Integration

Use SPS with One Identity Starling and take advantage of companion features from Starling products such as 2FA and Safeguard Remote Access.

Join status: Joined

Joined to Starling

This node is joined to Starling Services

Instance ID sps-master-6d3f3fca-334d-4ef1-86c7-0be5fb4ec5b0

Product Name Safeguard

Safeguard Remote Access

You can access your network from the Starling platform, using this Safeguard for Privileged Sessions appliance.

○ Enable Safeguard Remote Access

Result

Your SPS instance is joined to Starling.

Starling integration

One Identity Starling helps to combine products from the One Identity line to create a secure and customizable cloud service. For more information, see the Starling technical documentation.

If you are using a Starling 2FA plugin, (that is, you have uploaded it to **Basic Settings** > **Plugins** and then configured it at **Policies** > **AA Plugin Configurations**) and the SPS node is joined to One Identity Starling, you do not have to specify `api_key` and `api_url` in the Starling 2FA plugin configuration. This configuration method is more secure.

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

Glossary

C

Cadence icons

One Identity font that contains standard icons used in the user interfaces for various One Identity products.

Channel Policy

The channel policy lists the SSH channels (for example terminal session, SCP, and so on) that can be used in a connection. The channel policy can further restrict access to each channel based on the IP address of the client or the server, a user list, or a time policy.

D

Drop-down

Flare default style that can be used to group content within a topic. It is a resource to structure and collapse content especially in non-print outputs.

G

Glossary

List of short definitions of product-specific terms.

N

Note

Circumstance that needs special attention.

S

SaaS

Software-as-a-Service.

Skin

Used to design the online output window.

Snippet

Flare file type that can be used to reuse content. The One Identity SRA contains various default snippets.

SPS

Safeguard for Privileged Sessions

T

Tip

Additional, useful information.

Index