



One Identity Safeguard Remote Access

Quick Start Guide

Copyright 2021 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Contents

Introduction	5
Disclaimer	6
Prerequisites	7
Limitations	8
Getting started	9
Creating and signing in to a One Identity Starling account	9
Creating a new organization	9
Signing in to One Identity Starling	11
Starting the One Identity Safeguard Remote Access trial	12
Set up One Identity Safeguard for Privileged Sessions	12
User mapping policy	13
Credential store	13
Upload Authentication and Authorization plugin	14
Configure Authentication and Authorization plugin	17
Connection policy	17
HTTPS proxy	20
Starling join	20
Enable Safeguard Remote Access	21
Admin-side use cases	23
Admin web interface location	23
Inviting a Starling Collaborator	23
Adding a new connection to an existing target server	24
Setting the maximum RDP image resolution	25
User-side use cases	27
User web interface location	27
Connecting to the target server	27
Using the Session tab	28
Using the User Preference tab	29
Appendix	30

Configuring usermapping policies	30
Configuring local Credential Stores	32
Using credential stores for server-side authentication	35
Using plugins	36
Configuring connections	37
HTTPS proxy	44
Joining SPS to One Identity Starling	45
One Identity Starling integration	47
About us	48
Contacting us	48
Technical support resources	48
Glossary	49
Index	51

Introduction

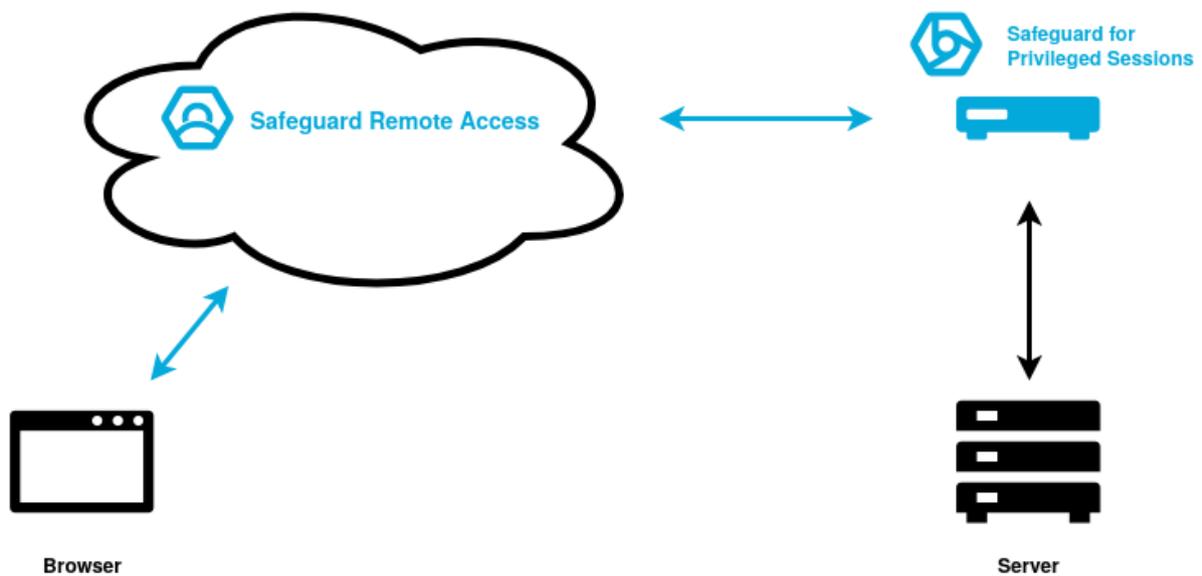
Intended Audience

For Administrators the One Identity Safeguard Remote Access Quick Start Guide contains information about how to set up One Identity Safeguard Remote Access in the One Identity Starling and how to integrate with One Identity Safeguard for Privileged Sessions. For Users this Quick Start Guide describes the usage and features of One Identity Safeguard Remote Access.

Overview

One Identity Safeguard Remote Access is a Cloud software as a service (SaaS) that provides a client-less, browser based secure terminal access to servers via integration with the One Identity Safeguard for Privileged Sessions product.

Figure 1: One Identity Safeguard Remote Access architecture overview



Disclaimer

The beta (preview) version of One Identity Safeguard Remote Access must be enabled and used in a test environment only. As it is a preview version, it is not ready to be used in a production environment.

For the most up-to-date version of this document, see [One Identity Safeguard Remote Access Beta Wiki](#).

Prerequisites

In order to set up One Identity Safeguard Remote Access, the following prerequisites must be met:

- One Identity Safeguard for Privileged Sessions version 6.9.0 and onward is installed and basic network configuration is completed, the web administrative interface is available.
- A Safeguard for Privileged Sessions Authentication and Authorization (AA) plugin is selected.

[Using plugins](#) on page 36

- Credential store is available for use in One Identity Safeguard for Privileged Sessions.

[Using credential stores for server-side authentication](#) on page 35

[Configuring local Credential Stores](#) on page 32

- The user has the role of Administrator under the Remote Access product in the One Identity Starling.

Limitations

This section introduces limitations to the preview version of One Identity Safeguard Remote Access.

Security-related limitations:

- Safeguard Remote Access stores and processes data in cloud services located in the United States.
- The user is not required to periodically re-authenticate to a running session. Once the user logged in to a terminal session, they stay logged in to One Identity Safeguard Remote Access.
- Targets cannot be hidden selectively.
- All target servers are visible to collaborators - no fine-grained access control over which user sees which server. (To be introduced by integration to AAD later.)
- The bandwidth usage of terminal connections is not limited.

Functionality-related limitations:

- Only SSH and RDP protocols are fully supported, VNC and Telnet on best effort basis.
- No RDP gateway supported, One Identity Safeguard Remote Access itself acts as the gateway.
- No RDP remote application or SCP over SSH supported at this time.
- Only fixed and inband destination selection defined in One Identity Safeguard for Privileged Sessions will be picked up by One Identity Safeguard Remote Access.
- One Identity Safeguard for Privileged Sessions nodes are not monitored. In case a One Identity Safeguard for Privileged Sessions fails, or it is unjoined from One Identity Starling and so on - the related target connections remain visible on One Identity Safeguard Remote Access.
- No Copy & Paste support in terminal sessions. (Work in progress for Chrome based browsers.)
- The server side resolution in terminal sessions cannot be changed.
- SSH sessions always require credential injection (that is Credential Store). (Bugfix in progress.)
- Inband target servers provided by the end user are currently not supported, only preset inband targets.

Getting started

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

Creating and signing in to a One Identity Starling account

This section describe 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 in order 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 **United States** (for the United States data center).
| **NOTE:** Only the United States data center is supported.
4. 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 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.

Figure 2: Try Starling - Creating your account

The screenshot shows a 'Create your Account' form. At the top, there is a user icon and a partially obscured email address ending in '.com', with a 'Not you?' link below it. The form contains the following fields: 'Organization Name' (with a redacted value), 'First Name' (with a redacted value), 'Last Name' (with a redacted value), and 'Phone Number' (with a redacted value and a country selector set to the United States). Below the fields is a checkbox that is checked, with the text 'I have read, I understand and I accept the Terms of Use, Privacy Policy, Software Transaction Agreement, and SaaS Addendum'. A blue 'START' button with a right-pointing arrow is located at the bottom right of the form.

NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States) 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 if 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).
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 eight to sixteen 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 associated with the requirement.
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 that is not associated with an existing work account.

To sign in to One Identity Starling

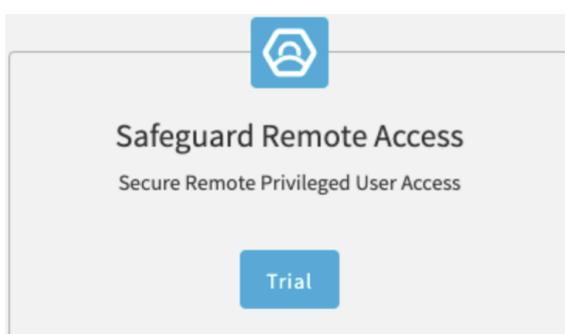
1. From the One Identity Starling home page (<https://www.cloud.oneidentity.com/>) click **Sign in to Starling**.
2. The next steps will depend on whether or not you have previously stored login information.
 - If signing in to One Identity Starling using a browser that has not previously stored login information:
 1. Select United States (for the United States 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 (United State) to reselect your data center region. This will restart the process for storing your login information.
 4. Enter your password then click **SIGN IN**.
You are now signed in to One Identity Starling.
 - 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 (United States) to reselect your data center region. Follow the steps provided above for a browser that has not previously stored login information.
 2. Once One Identity Starling has confirmed there is no work account associated with your email address, a password prompt will appear. Enter your password then click **SIGN IN**.
You are now signed in to One Identity Starling.

Starting the One Identity Safeguard Remote Access trial

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.

Set up One Identity Safeguard for Privileged Sessions

This section describes the various settings, policies to be set up in One Identity Safeguard for Privileged Sessions in order to join the appliance to One Identity Starling and integrate with One Identity Safeguard Remote Access.

The configuration pages referenced in this section are applicable to the Web UI interface of One Identity Safeguard for Privileged Sessions and are written in bold. For example, **Basic Settings > Network**.

- [User mapping policy](#)
- [Credential store](#)

- [Upload Authentication and Authorization plugin](#)
- [Configure Authentication and Authorization plugin](#)
- [Connection policy](#)
- [HTTPS proxy](#)
- [Starling join](#)
- [Enable Safeguard Remote Access](#)

User mapping policy

In a One Identity Safeguard Remote Access use case the end-user and the user on the (target) server is usually different. The end-user is identified by their email address and the server user is typically an administrative account name like root or Administrator. One Identity Safeguard for Privileged Sessions does not allow different end-user (called gateway user in One Identity Safeguard for Privileged Sessions) and server user by default in a connection. Therefore a Usermapping policy is required to be applied on the connection policy.

Navigate to **Policies > Usermapping policies**, and add a new policy (username and group). For example a policy that allows any kind of user mapping (for example, * → all).

Figure 4: Policies > Usermapping policies - Creating usermapping policies

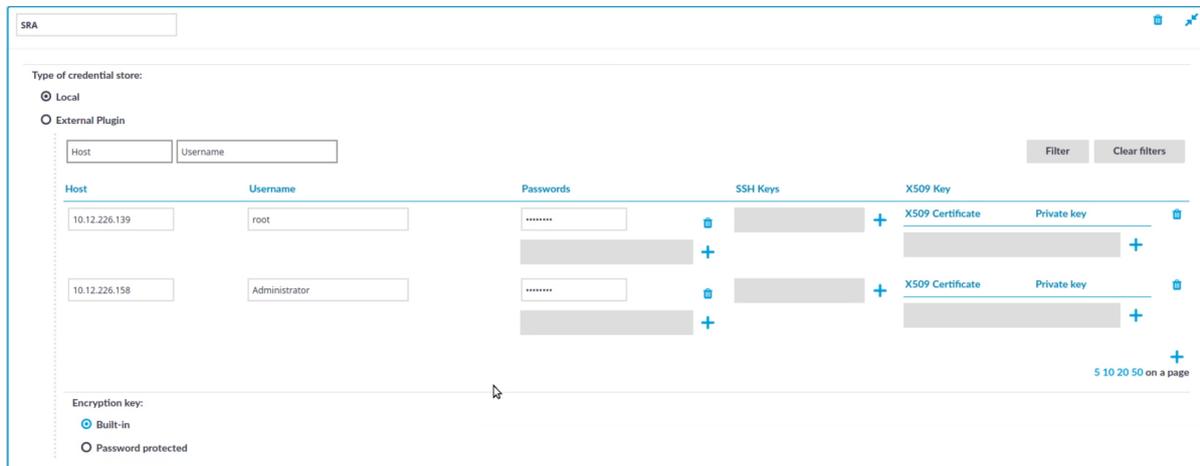
For more information on HTTPS proxy setting, refer to the [One Identity Safeguard for Privileged Sessions Administration Guide](#) or part of it in [Configuring usermapping policies](#) on page 30 in the Appendix.

Credential store

For RDP this step is optional, for SSH it is currently mandatory.

To enable password-less login to target servers, set up a credential store. For example, create a local credential store and setup up login credentials to the target server.

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



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 32 and [Using credential stores for server-side authentication](#) on page 35 in the Appendix.

Upload Authentication and Authorization plugin

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

In the One Identity Safeguard Remote Access 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 One Identity Safeguard for Privileged Sessions the end-user authentication is called gateway authentication. Gateway authentication is required to be able to audit the end-user. One Identity Safeguard for Privileged Sessions can delegate the gateway authentication to One Identity Safeguard Remote Access if a suitable AA plugin is in used.

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-test-1>

Figure 6: Downloading the AA plugin

The screenshot shows a GitHub release page for the `SPS_AA_Skeleton-1.1.0-test-1` plugin. The release is labeled as a **Pre-release** and was released by `krajorama` 12 minutes ago. The build information states: "Minimal compatible SPS version is 6.3.0. Built with Plugin SDK version 1.4.4." The SHA256 checksum is `6ed1ae7c1987f32f40314156c95fb20ff01fd1b6ecec7ce7563a8b7db5e3a7f SPS_AA_Skeleton-1.1.0-test-1.zip`. The assets section lists four items: `SPS_AA_Skeleton-1.1.0-test-1.zip` (134 KB), `SPS_AA_Skeleton-1.1.0-test-1.zip.sha256.txt` (97 Bytes), `Source code (zip)`, and `Source code (tar.gz)`.

Download the first ZIP file.

- Use an official AA plugin that does Multi Factor Authentication:

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

or from Github:

<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 the **Upload plugin** bar.

As a result the plugin is shown like this:

Figure 7: Uploading the plugin

The screenshot shows a web browser window with the URL `https://zts-scb-31.scb.balabit/portal/#/config/basic/plugins`. The browser's address bar and tabs are visible at the top. Below the browser window, there is a blue header with the text "ed Sessions".

The main content area is divided into two columns:

- Uploaded plugins:** A list of plugins. The first plugin is "SPS_AA_Skeleton" with the description "Authentication and Authorization" and "This is an example Python3 AA plugin". The version is "1.1.0-20210203T093150".
- Plugin details:** A detailed view of the "SPS_AA_Skeleton" plugin. It includes the following information:
 - Authentication and Authorization:** SPS_AA_Skeleton, Version: 1.1.0-20210203T093150. Description: 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:** A "Check Integrity" button.
 - SHA256 checksum:** `edaf75d7299d3c382121f112b1499aed41623e8ca862db6b409392f758eabba2`.
 - Copy:** A section with instructions: "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** and **Delete** buttons.

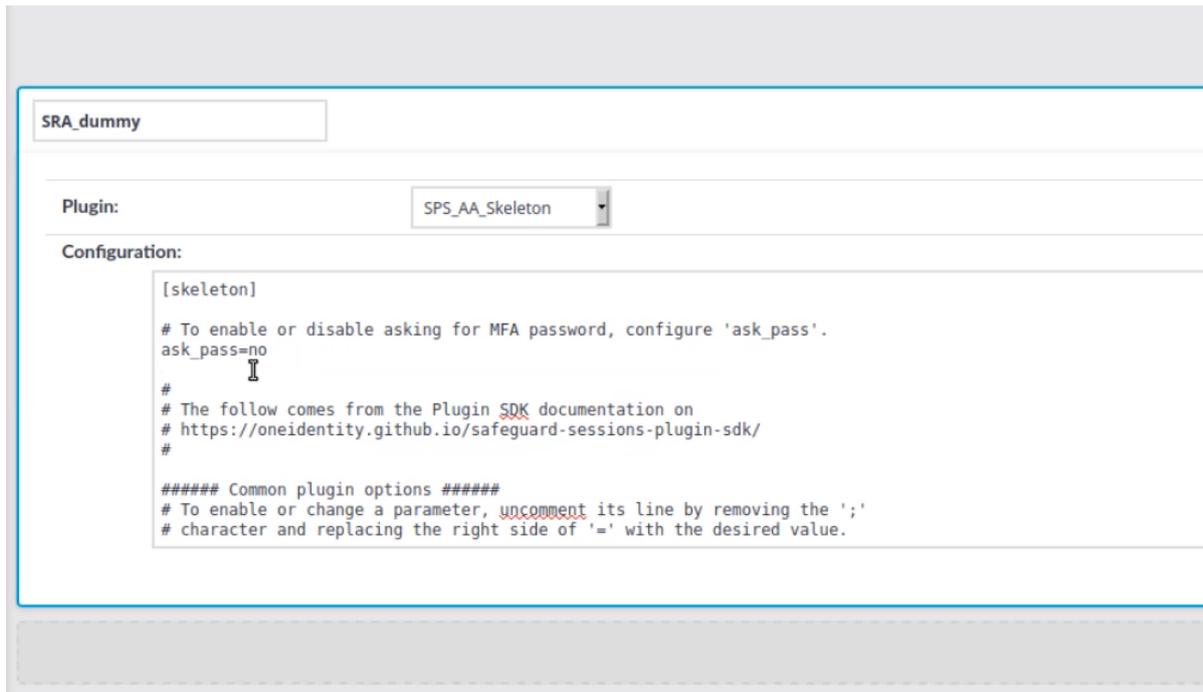
For more information on HTTPS proxy setting, refer to the [One Identity Safeguard for Privileged Sessions Administration Guide](#) or part of it in [Using plugins](#) on page 36 in the Appendix.

Configure Authentication and Authorization 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



The screenshot shows a configuration window for an SRA dummy. At the top, there is a text input field containing "SRA_dummy". Below this, there is a "Plugin:" label followed by a dropdown menu showing "SPS_AA_Skeleton". Underneath, there is a "Configuration:" label followed by a text area containing the following configuration text:

```
[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.
```

Connection policy

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

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 in case the target of the connection policy is a fixed address. In the case of inband target selection the name is shown 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 9: Setting the name and target address of the connection policy

The screenshot displays a configuration interface for a connection policy named `linux_servers`. At the top, there are three tabs: `Backup ALL`, `Restore ALL`, and `Archive/cleanup ALL`. Below the tabs, the policy is configured with the following details:

- Name:** `linux_servers`
- From:** `0.0.0.0 / 0` and `:: / 0`
- To:** `0.0.0.0 / 0` and `:: / 0`
- Port:** `2222`

The **Target:** section includes the following options:

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

Under **Inband destination selection**, there are two sub-sections:

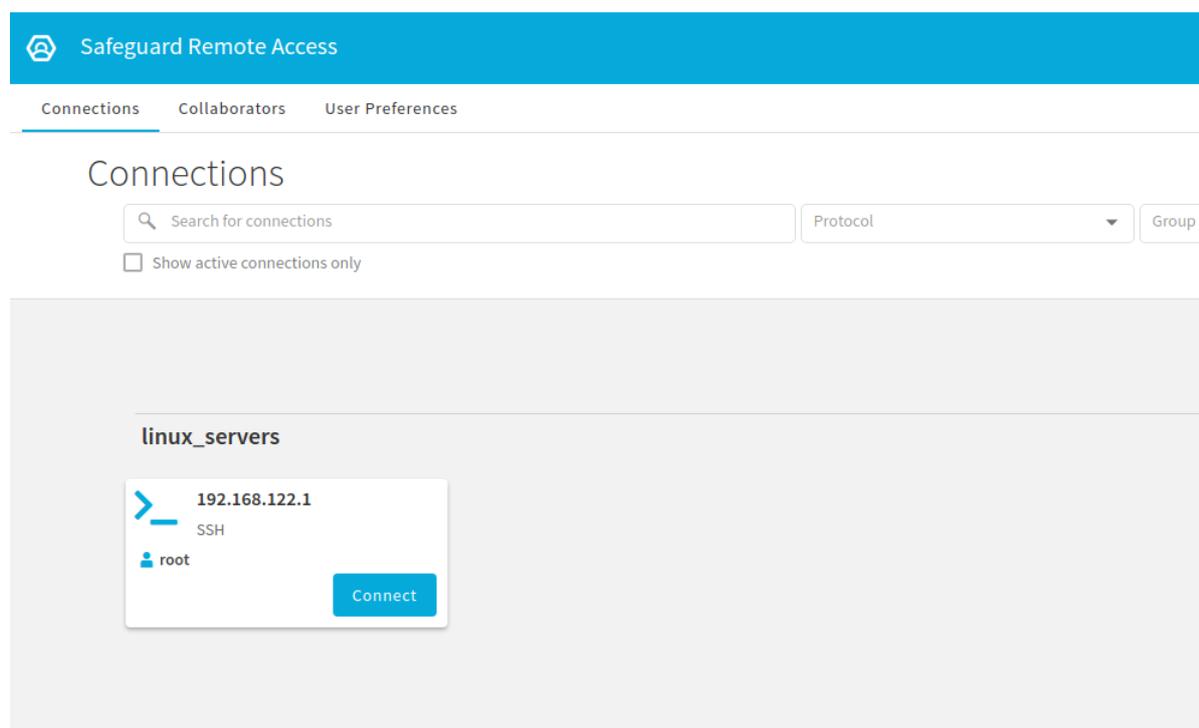
- Targets:** A table with columns `Domain` and `Port`. One entry is visible: `192.168.122.1` with port `22`. A plus sign (+) is next to the table to add more targets.
- Exceptions:** A table with columns `Domain` and `Port`. It is currently empty, with a plus sign (+) next to the table to add exceptions.

Below the targets and exceptions, there is an **Append domains:** section with a `Domain` input field and a plus sign (+) to add domains.

At the bottom, there is a checkbox labeled **Enable Custom Target DNS server:** which is currently unchecked.

and `linux_servers` became the group containing one connection towards the `192.168.122.1` target.

Figure 10: 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 may be anywhere on the internet, thus this field should be filled with `0.0.0.0/0` to cover all IPv4 clients.

NOTE: In order 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 in order to introduce 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 to `0.0.0.0/0` also to allow automated handling of this parameter.

Target

Only the choices **Use fixed address** and **Inband destination selection** are compatible with SRA. In case of inband destination selection, only those target domains (bit of a misnomer) will be shown on connection tiles that specify specific IPv4 or IPv6 addresses or contain a hostname. Subdomains, networks are ignored.

Policies

Use the previous AA plugin configuration, credential store and user mapping policy - everything else can be default or user defined.

Figure 11: 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 HTTPS proxy setting, refer to the [One Identity Safeguard for Privileged Sessions Administration Guide](#) or part of it in [Configuring connections](#) on page 37 in the Appendix.

HTTPS proxy

One Identity Safeguard for Privileged Sessions needs HTTPS access to One Identity Safeguard Remote Access in the cloud. In case the One Identity Safeguard for Privileged Sessions appliance has no direct connectivity to the internet (for example is behind firewalls), you can set a HTTPS proxy in **Basic Settings** > **Network** configuration page.

For more information on HTTPS proxy setting, refer to the [One Identity Safeguard for Privileged Sessions Administration Guide](#) or part of it in [HTTPS proxy](#) on page 44 in the Appendix.

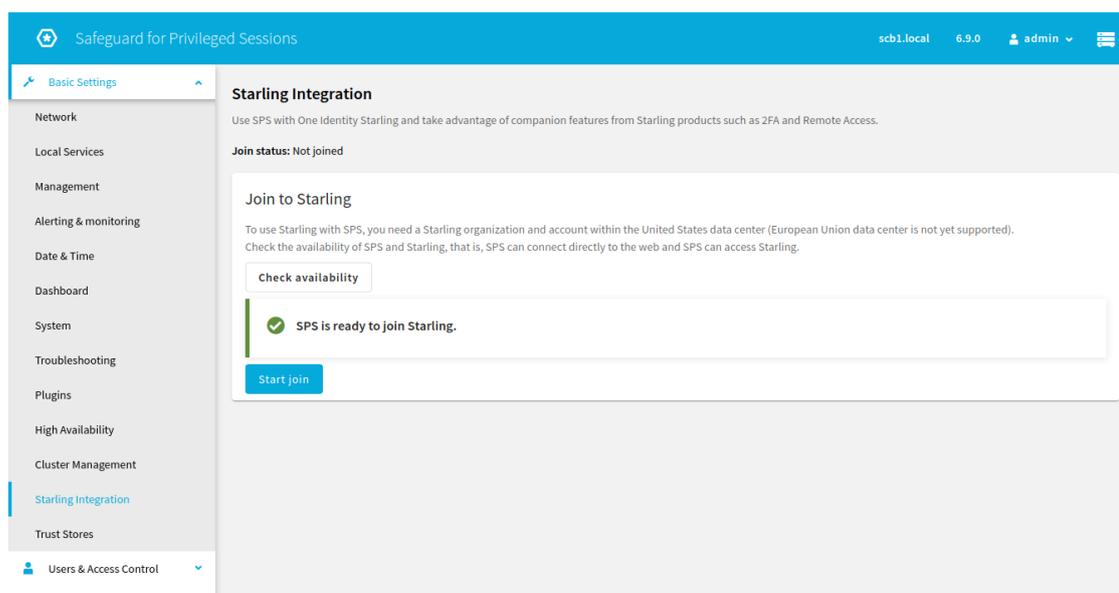
Starling join

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

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

| **NOTE:** If asked, choose the US data center.

Figure 12: Join to Starling



For more information on HTTPS proxy setting, refer to the [One Identity Safeguard for Privileged Sessions Administration Guide](#) or part of it in [Joining SPS to One Identity Starling](#) on page 45 in the Appendix.

Enable Safeguard Remote Access

1. Navigate to **Basic Settings > Starling Integration > Remote Access > Enable Remote Access**.
2. Simply toggle the switch to enable One Identity Safeguard Remote Access.
3. On the One Identity Safeguard Remote Access home page your connections should now be listed with default accounts (root for SSH and Administrator for RDP).

Figure 13: 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 Safeguard
Name

[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

Admin-side use cases

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

Admin 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 is loaded from the One Identity Safeguard Remote Access 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.

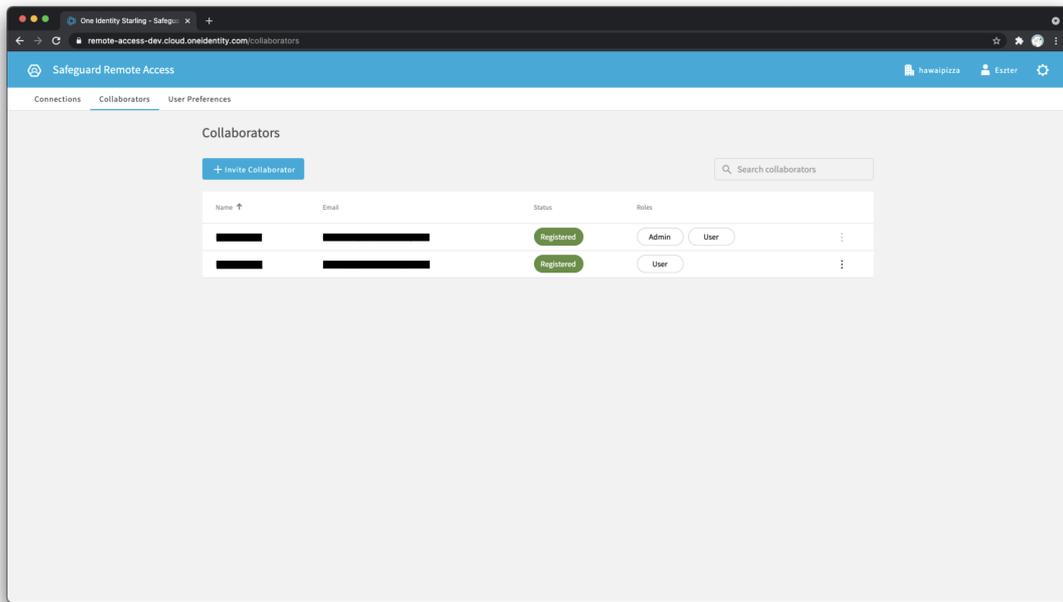
Inviting a Starling Collaborator

Inviting a collaborator makes is possible for multiple people to work simultaneously on a project.

To invite a Starling Collaborator with the User role

1. Navigate to the **Collaborators** tab.
2. Click on the **Invite Collaborator** bar.

Figure 14: Inviting a Starling Collaborator



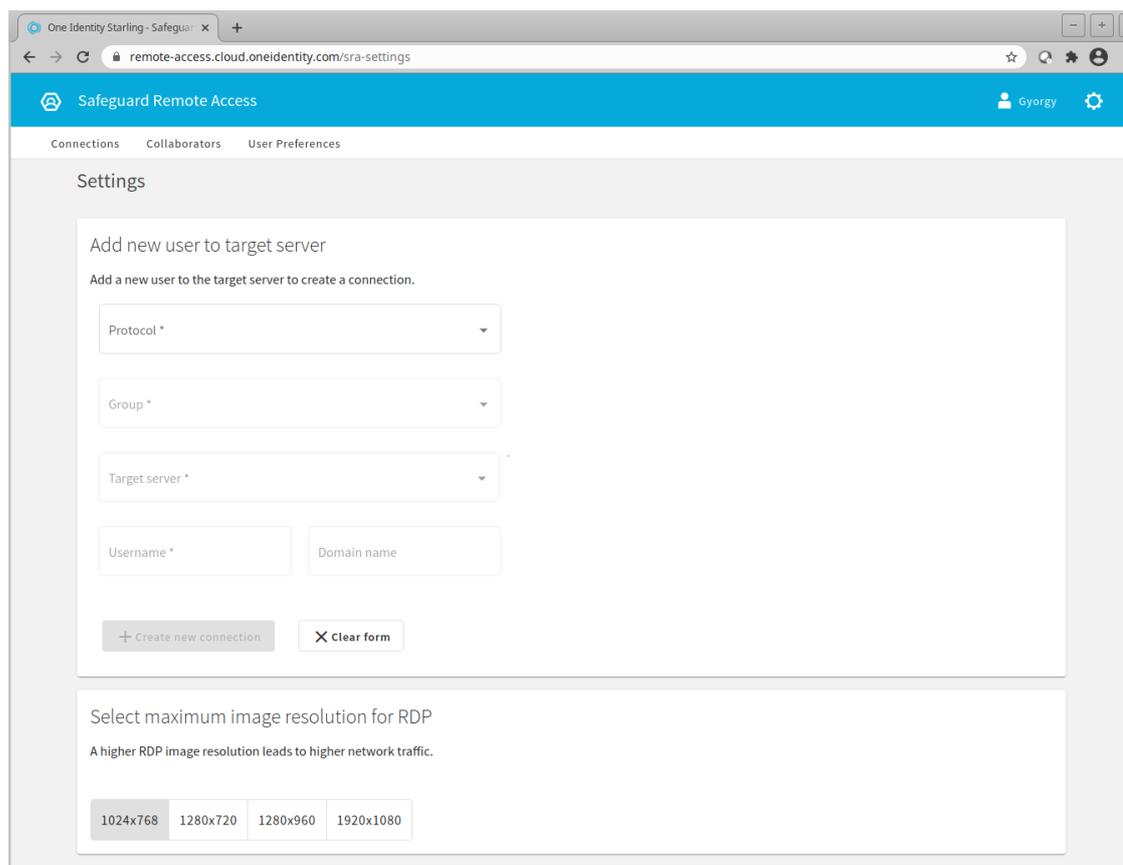
Adding a new connection to an existing target server

Each target server can serve multiple connections. These connections can be grouped based on various attributes, such as the applied protocol (RDP or SSH), the group name, or the name of the target server.

To add a new connection to an existing target server

1. Click the Settings icon and select **Remote Access Settings**.
2. Under **Settings**, click on **Add new user to target server**.

Figure 15: Adding a new user to the target server



3. Specify the protocol, the group, and the target server of the new connection.
4. Specify a username and a domain name. (The domain name is optional.)
5. Click the **Create new connection** bar.

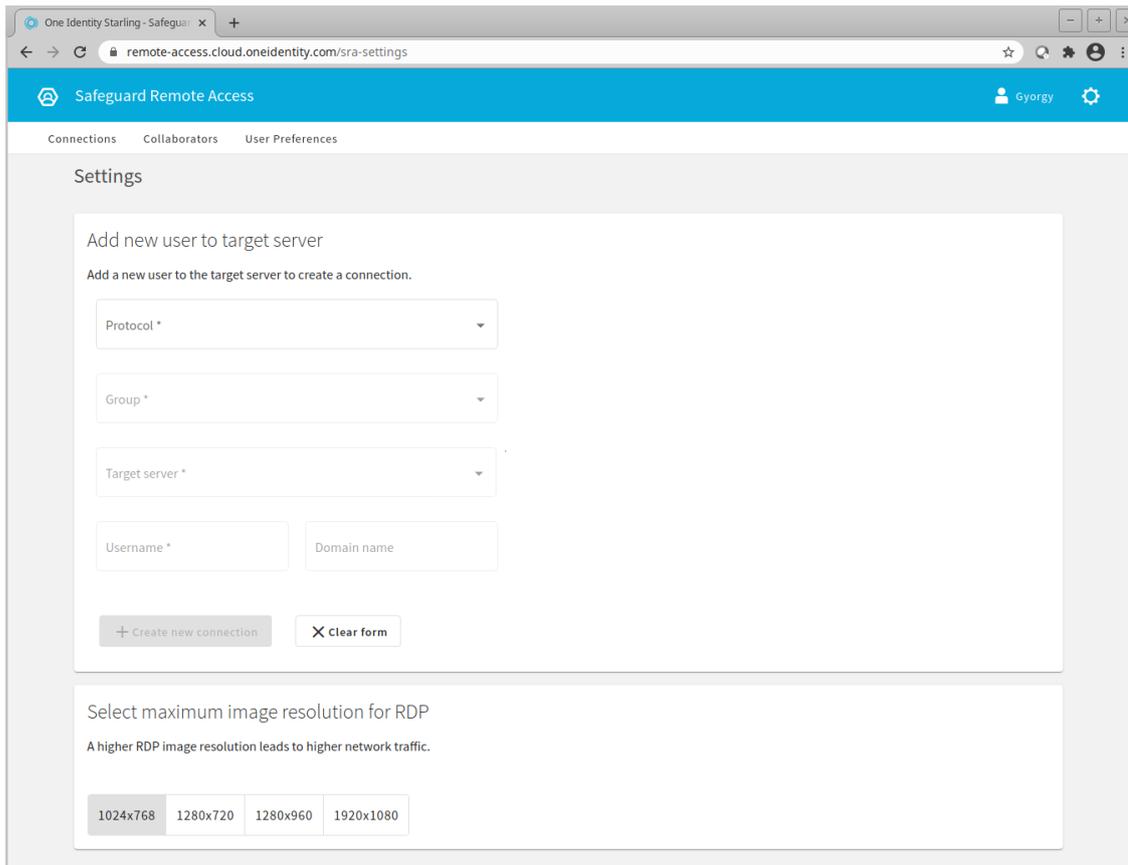
Setting the maximum RDP image resolution

Setting the RDP image resolution results in a better stream quality.

NOTE: A higher RDP image resolution leads to higher network traffic.

To set the maximum RDP image resolution:

1. Click the Settings icon and select **Remote Access Settings**
2. Under **Settings**, find **Select maximum image resolution for RDP** at the bottom.



3. Click on the preferred image resolution.
The default value is **1024x768**.

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.

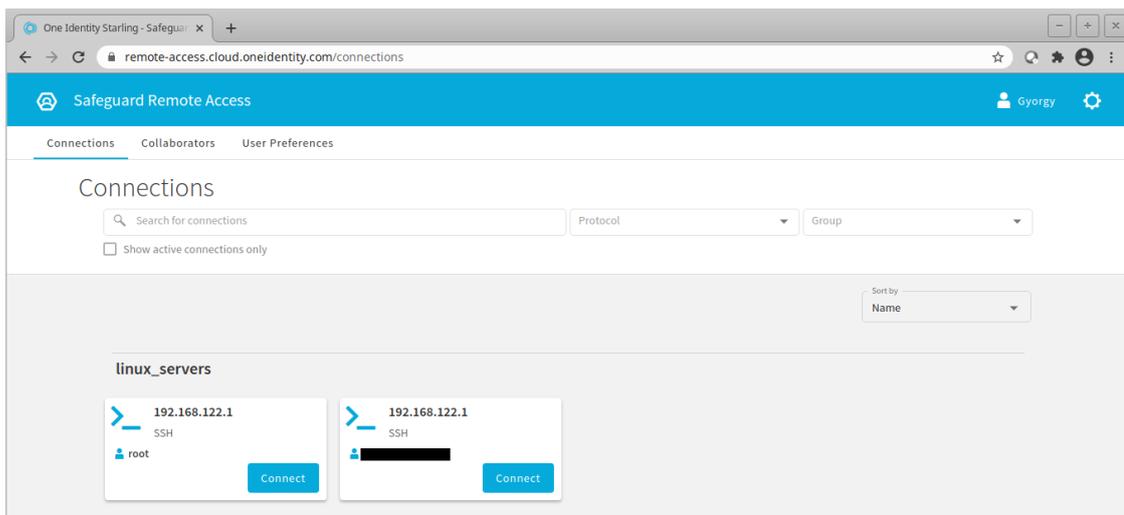
The contents of the interface is loaded from the One Identity Safeguard Remote Access subscription where the User is an Administrator or User. If the user is member of multiple subscriptions, then the appropriate subscription can be selected in the upper right corner.

Connecting to the target server

To connect to the target server

1. Navigate to the **Connections** tab at the top left corner of the page.
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 16: Connecting to the target server



4. A new browser will open, wait until the connection is established to the target server.

Using the Session tab

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 three menu icons:

- End session

Clicking on the X button will disconnect you from the target server. Alternatively, clicking on the One Identity Safeguard Remote Access icon 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.

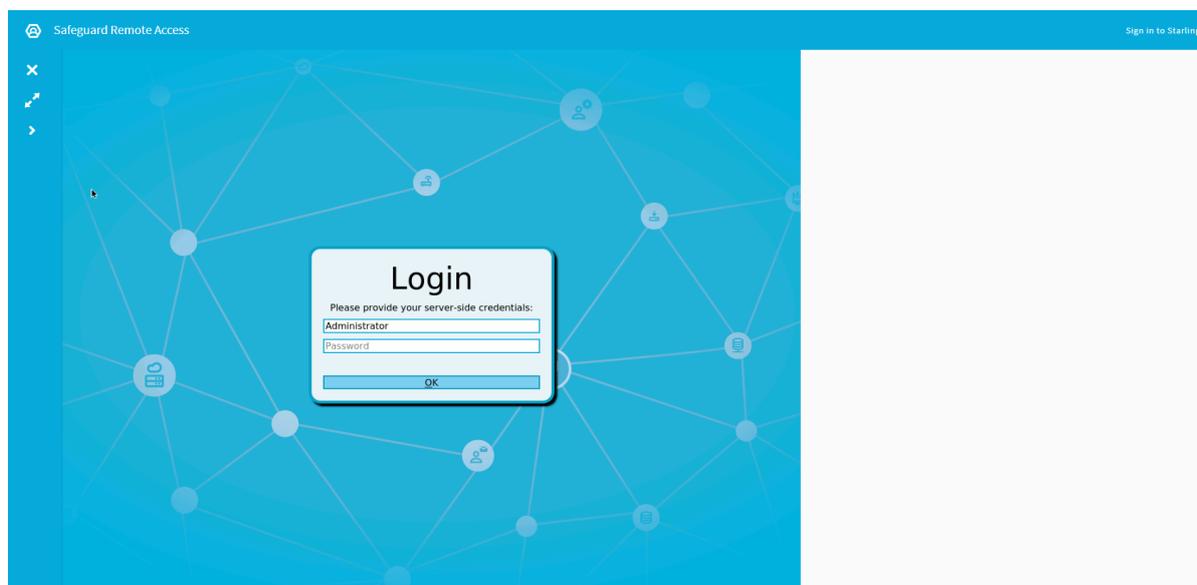
- Enter fullscreen mode

To exit the fullscreen mode, press **Esc**.

- Close control panel

Open or close the control panel on the left side.

Figure 17: Using the Session tab



Using the User Preference tab

Set the default RDP image resolution

Setting the RDP image resolution results in a better stream quality.

NOTE: Available choices may be limited by the Administrator.

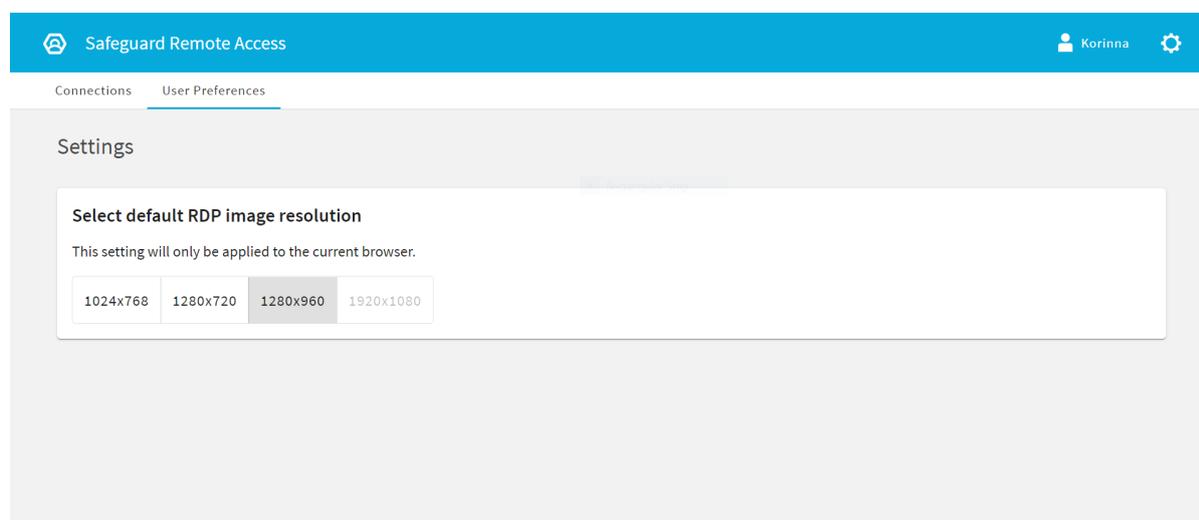
To set the default RDP image resolution:

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

The default value is **1024x768**.

The setting can be applied only to the current browser.

Figure 18: Setting the default RDP image resolution



Appendix

This section covers 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 user name to access the remote server: only members of the specified local or LDAP usergroups (for example, administrators) can use the specified user name (for example, root) on the server.

- ⚠ **CAUTION:** In SSH connections, the users must use the following as their user name: `gu=username@remoteusername`, where `username` is the user name used in the LDAP directory, SPS will use this user name to determine their group memberships, and `remoteusername` is the user name 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 user name of SSH users, only valid UTF-8 strings are allowed.

- ⚠ **CAUTION:** In Telnet connections, usermapping policy works only if Extract user name from the traffic is enabled.

For more information, see [Extracting username from Telnet connections](#).

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 user name used to access the remote server. Therefore, you need to enable usermapping to the `Anon*` user names.

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.

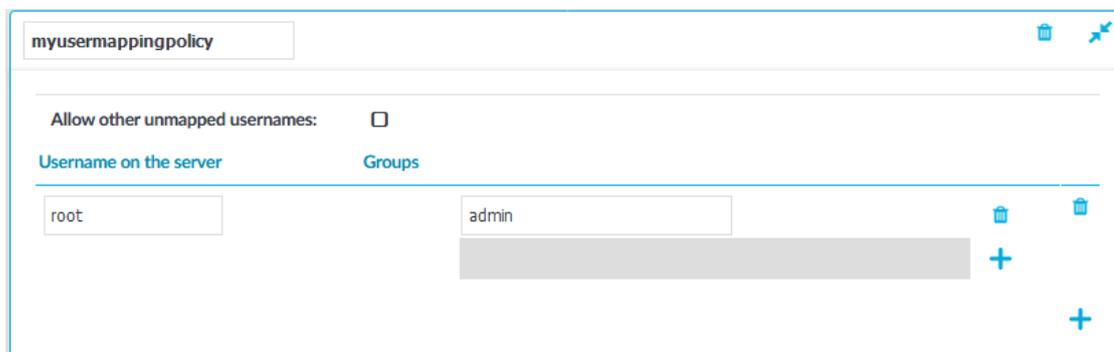
For more information on using usermapping policies, see [Configuring usermapping policies](#).

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 19: Policies > Usermapping Policies — Configuring usermapping policies



2. Click **+** to create a new policy, and enter a name for the policy.
3. Click **+** and enter the user name that can be used to access the remote server (for example root) into the **Username on the server** field. SPS will use this user name in the server-side connection. To permit any user name on the server side, enter an asterisk (*).
4. Select **Groups**, click **+** and specify who is permitted to use the remote user name 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 user group (for example admins) whose members will be permitted to use the remote user name.
For more information on LDAP authentication, see [Authenticating users to an LDAP server](#).

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 user list whose members will be permitted to use the remote user name.
For more information on using user lists, see [Creating and editing user lists](#).

Repeat this step to add further groups if needed.
5. Repeat steps 3-4 to add further user names 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 user name 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.

Commit

10. Click

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

When configuring usermapping for RDP connections, proceed to [Configuring out-of-band gateway authentication](#) and configure gateway authentication.

When configuring usermapping for RDP connections, proceed to [Configuring out-of-band gateway authentication](#) in the *One Identity Safeguard for Privileged Sessions Administration Guide* and 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 One Identity Safeguard for Privileged Sessions (SPS) using gateway authentication or an AA plugin. Therefore gateway authentication or an AA plugin must be configured for these connections.

For more information, see [and](#) .

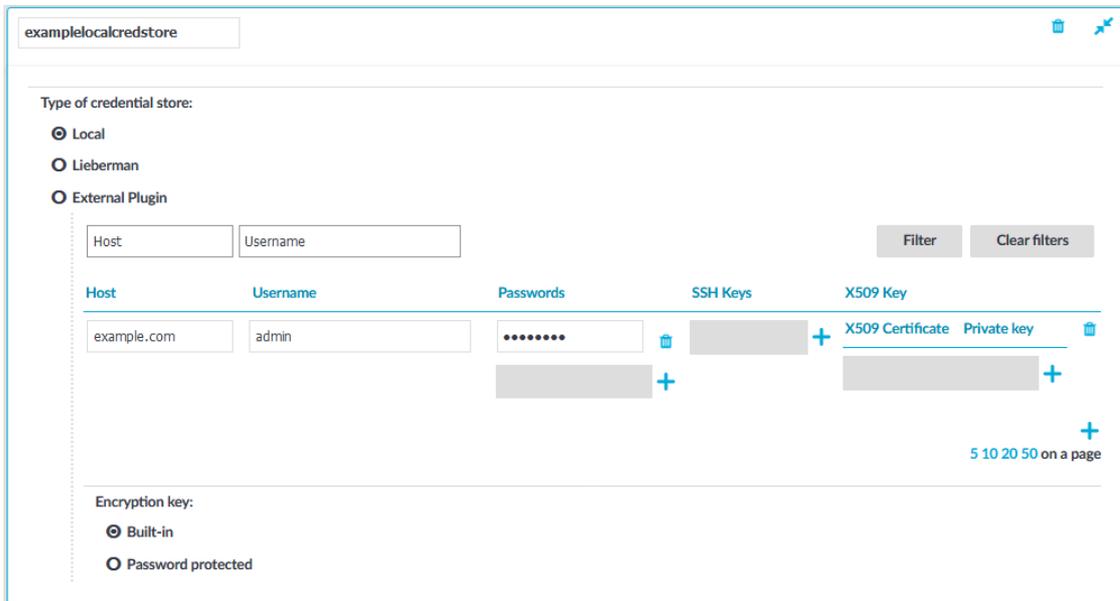
To configure a local Credential Store that stores the credentials used to login to the target host

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.

To use custom passwords to encrypt the Credential Store, see [Configuring password-protected Credential Stores](#).

To use custom passwords to encrypt the Credential Store, see [Configuring password-protected Credential Stores](#) in the *One Identity Safeguard for Privileged Sessions Administration Guide*.

Figure 20: Policies > Credential Stores > Local – Configuring local Credential Stores



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:

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: One Identity Safeguard for Privileged Sessions (SPS) accepts passwords that are not longer than 150 characters. Letters A-Z, a-z, numbers 0-9, the space character, as well as the following special characters can be used: !"#%&'()*+,-./:;<>=?@[]\^_`{|}_|

- 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](#).

7. Click  .
8. Navigate to the Connection policy where you want to use the Credential Store (for example, to **SSH Control > Connections**), select the Credential Store to use in the

Credential Store field, then click  .

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 21: <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:	<input type="checkbox"/>		

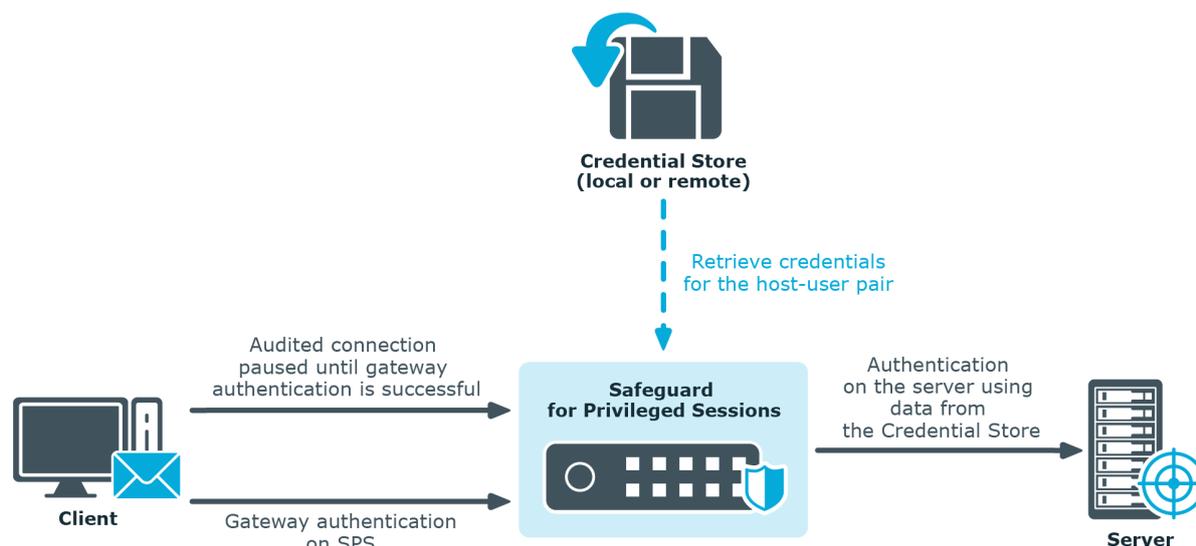
Using credential stores for server-side authentication

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 One Identity Safeguard for Privileged Sessions (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.

For more information on gateway authentication, see [Configuring gateway authentication](#).

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

Figure 22: 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.

- To configure a local Credential Store, see [Configuring local Credential Stores](#).
- To configure a local, password-protected Credential Store, see [Configuring password-protected Credential Stores](#).
- To unlock a local, password-protected Credential Store, see [Unlocking Credential Stores](#).
- To configure a custom Credential Store plugin, see [Using a custom Credential Store plugin to authenticate on the target hosts](#).

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.

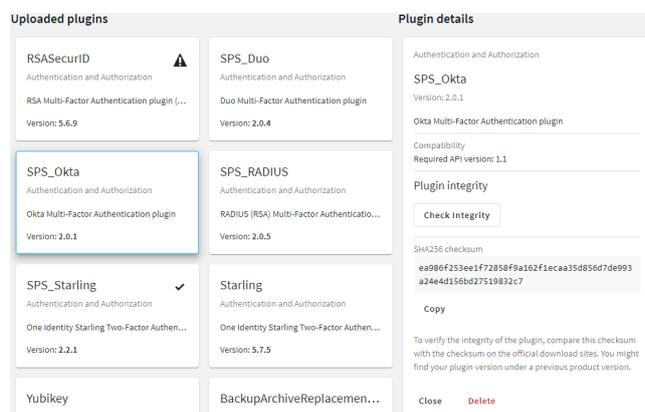
In case of authenticating to RDP servers using Network Level Authentication (NLA), the server-side password is prompted at the start of the connection. If there is no password in the credential store for the user and the server-side password is incorrect, the connection is terminated.

Using plugins

To download the official plugins for your product version, navigate to [the product page on the Support Portal](#). The official plugins are also available on [GitHub](#).

To write your own custom plugin, feel free to use our [Plugin SDK](#).

Figure 23: Basic Settings > Plugins — Viewing the uploaded plugins



The following plugin types can be uploaded to SPS:

- Authentication and Authorization plugins
For more information, see [Integrating external authentication and authorization systems](#).
- Credential Store plugins

For more information, see [Using a custom Credential Store plugin to authenticate on the target hosts](#).

- Configuration Synchronization plugins

For more information, see [Using a configuration synchronization plugin](#).

- Signing CA plugins

For more information, see [Signing certificates on-the-fly](#).

For more information about how to create an external Signing CA plugin, see [Creating an external Signing CA](#) in the *One Identity Safeguard for Privileged Sessions Administration Guide*.

Configuring connections

The following describes how to configure connections.

NOTE:

When configuring HTTP or SSH connections, avoid using the IP address configured for administrator or user login on One Identity Safeguard for Privileged Sessions (SPS).

To configure connections

1. Select the type of connection from the main menu.
 - To configure a 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 will identify the connection (for example admin_mainserver).

TIP: It is recommended to 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 24: <Protocol name> Control > Connections – Configuring connections

Enabled	Name	From	To	Port
<input checked="" type="checkbox"/>	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
 - Allow fallback to legacy RDP Security Layer

Act as a Remote Desktop Gateway:

Verify server certificate:

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:

Indexing policy:

Connection rate limit: connections/minute/client

Delete search metadata from SPS after: days

If you do not set this option here, the same option under Global Options takes effect.

RDP settings:

Channel policy:

Audit policy:

LDAP server:

Usermapping policy:

Backup policy:

Archive/Cleanup policy:

Analytics policy:

Credential Store:

AA plugin:

Require Gateway Authentication on the SPS Web Interface:

Access Control:
Configure search 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:

- Enter the IP address of the client that will be permitted to access the server into the **From** field. Click to list additional clients.

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 also enter a hostname instead. One Identity Safeguard for Privileged Sessions (SPS) automatically resolves the hostname to an IP address.

NOTE: Note the following limitations:

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

4. Enter the IP address that the clients will request into the **To** field.

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 also enter a hostname instead. One Identity Safeguard for Privileged Sessions (SPS) automatically resolves the hostname to an IP address.

NOTE: Note the following limitations:

- SPS uses the Domain Name Servers set in the **Basic Settings > Network > Naming > Primary DNS server** and **Secondary DNS server** fields to resolve the hostnames.
- If the Domain Name Server returns multiple IP addresses, SPS selects randomly from the list.
- In non-transparent mode, enter the IP address of a SPS logical interface. For more information on setting up logical network interfaces on SPS, see [Managing logical interfaces](#).
- In transparent mode, enter the IP address of the protected server.

Click  to add additional IP addresses.

5. If the clients use a custom port to address the server instead of the default port used by the protocol, enter the port number that the clients will request into the **Port** field.

Click  to list additional port numbers.

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

6. *Non-transparent mode:* Enter the IP address and port number of the target server into the **Target** field. SPS will connect all incoming client-side connections to this server.

For more information on organizing connections in non-transparent mode, see [Organizing connections in non-transparent mode](#).

Figure 25: <Protocol name> Control > Connections — Configuring non-transparent connections

Enabled	Name	From	To	Port
<input checked="" type="checkbox"/>	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. Configure advanced settings if needed, like network address translation, channel policy, gateway authentication, various policies, or other settings.

8. Click **+** to save the connection.

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

9. If needed, reorder the list of the connection policies. You can move connection policies by clicking the **^** and **v** buttons.

One Identity Safeguard for Privileged Sessions (SPS) compares the connection policies to the parameters of the connection request one-by-one, starting with the first policy in the policy list. The first connection policy completely matching the connection request is applied to the connection.

10. Depending on your needs and environment, you may want to set further settings for your connections.

- For details on modifying the destination or source addresses of the connections, see [Modifying the destination address](#) and [Modifying the source address](#).

For details on modifying the destination or source addresses of the connections, see [Modifying the destination address](#) and [Modifying the source address](#) in the *One Identity Safeguard for Privileged Sessions Administration Guide*.

- Select a **Backup Policy** and an **Archiving Policy** for the audit trails and indexes of the connection.

For more information on creating backup and archive policies in [Data and configuration backups](#) and [Archiving and cleanup](#).

If you have indexed trails, the index itself is also archived:

When using the **Indexer service**: Every 30 days, unless the **Backup & Archive/Cleanup > Archive/Cleanup policies > Delete data from SPS after** is configured to occur less frequently (more than 30 days). For example, if the **Delete data from SPS after** is 60 days, the index will be archived every 60 days. The content of the archived index will be the content that was available X days before the archival date, where X is the number in the **Delete data from SPS after** field.

CAUTION: Hazard of data loss Make sure you also backup your data besides archiving (for more information, see [Data and configuration backups](#)). If a system crash occurs, you can lose up to 30 days of index, since the index is only archived in every 30 days.

NOTE: The backup and archive policies set for the connection operate only on 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.

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

For more information, see [Audit policies](#).

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, you are recommended to encrypt the upstream traffic in the audit trail using a separate certificate from the downstream traffic.

For more information, see .

- To require the users to authenticate themselves not only on the target server, but on SPS as well, see [Configuring gateway authentication](#).
To require the users to authenticate themselves not only on the target server, but on SPS as well, see [Configuring gateway authentication](#) in the *One Identity Safeguard for Privileged SessionsAdministration Guide*.
- To require four-eyes authorization on the connections, with the possibility of an auditor monitoring the connection in real-time, see [Configuring four-eyes authorization](#).
To require four-eyes authorization on the connections, with the possibility of an auditor monitoring the connection in real-time, see [Configuring four-eyes authorization](#) in the *One Identity Safeguard for Privileged SessionsAdministration Guide*.
- In the case of certain connections and scenarios (for example SSH

authentication, gateway authentication, Network Level Authentication (NLA connections), SPS can authenticate the user to an LDAP database, or retrieve the group memberships of the user. To use these features, select an **LDAP Server**.

For more information, see [Authenticating users to an LDAP server](#).

NOTE:

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

- To limit the number of new connection requests accepted from a single client IP address per minute, enter the maximal number of accepted connections into the **Connection rate limit** field.

NOTE: Protocol-specific configuration options are described in their respective sections: [HTTP-specific settings](#), [ICA-specific settings](#), [RDP-specific settings](#), [SSH-specific settings](#), [Telnet-specific settings](#), and [VNC-specific settings](#).

11. If your clients and servers support it, configure the connection to use strong encryption.
 - For HTTP connections, see [Enabling TLS encryption in HTTP](#).
 - For Citrix ICA connections, use the following scenario: [Client - Broker - original secure gateway - Secure Ticket Authority \(STA\) - SRA - Server](#).
 - For RDP connections, see [Enabling TLS-encryption for RDP connections](#).
 - For SSH connections, see [Creating and editing protocol-level SSH settings](#).
 - For Telnet connections, see [Enabling TLS-encryption for Telnet connections](#).
 - For VNC connections, see [Enabling TLS-encryption for VNC connections](#).
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. Disable antialiasing in order to properly index the trails of these connections.

Note that antialiasing is enabled by default on Windows Vista and newer. Antialiasing is also called font smoothing. ClearType is an antialiasing technology used on Microsoft Windows, and should be disabled for optimal performance.

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

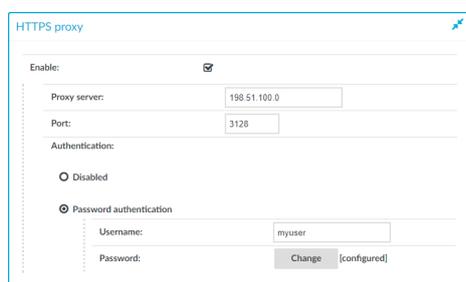
To ensure that your users can access the target servers only when their username is recorded, see [Usernames in RDP connections](#).

To ensure that your users can access the target servers only when their username is recorded, see [Usernames in RDP connections](#) in the *One Identity Safeguard for Privileged Sessions Administration Guide*.

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 26: Basic Settings > Network > HTTPS proxy



- **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

The following describes how to use SPS with One Identity Starling and take advantage of companion features from One Identity Starling products such as Starling Two-Factor Authentication and Identity Analytics.

Prerequisites

- An existing One Identity Starling organization (tenant)

NOTE: Consider the following:

- If you have several One Identity Starling organizations, you can join your SPS to any of the existing organizations, however, ensure that you remember the One Identity 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 One Identity Starling organization.
- To use One Identity Starling with SPS, you need a One Identity Starling organization and account within the 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 One Identity Starling integration on the Central Management node.

2. To check the availability of SPS and Starling, that is, SPS can connect directly to the web and SPS can access One Identity 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 One Identity Starling.

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

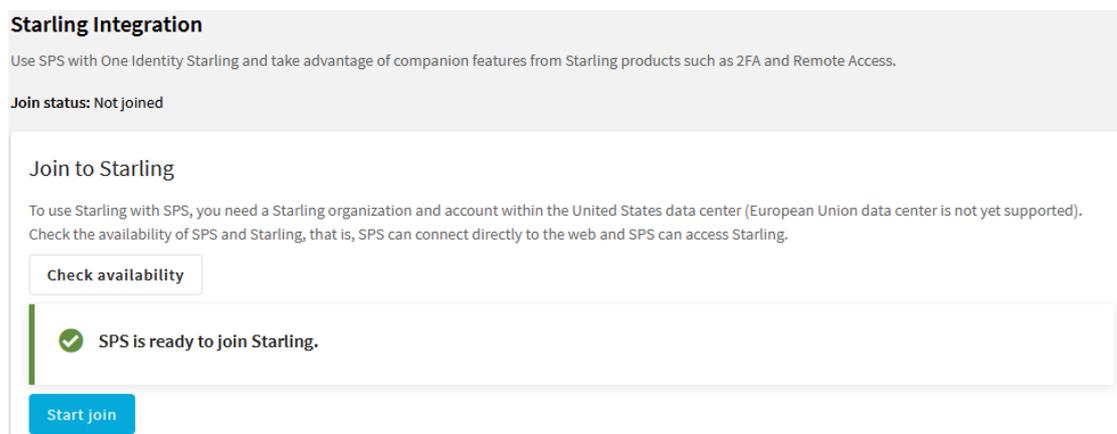
For more information, see [Network settings](#).

NOTE:

Currently only built-in Certificate Authorities are supported. If 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 One Identity Starling.

Figure 27: Basic Settings > Starling Integration — SPS is ready to join Starling



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

NOTE: Once you click **Start join**, you cannot stop the process and your SPS machine will be joined to One Identity Starling.

Ensure that you continue with the join process, and once the join process is complete, if required, you can unjoin SPS from One Identity Starling.

For more information, see [Unjoining SRA from One Identity Starling](#).

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

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

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

5. Copy your **Credential String** from the page.

The credential string allows SPS to communicate with One Identity Starling.

6. Navigate back to the SPS tab.

7. Paste your credential string into the **Credential string** field.

NOTE: If for some reason you cannot paste the credential string, you can re-retrieve it by refreshing this page and repeating the join process. You will receive the same credential string if you did not change your host name.

8. To complete the join process, click **Save & finish joining**.

Result

Your SPS instance is joined to One Identity Starling.

Figure 28: Basic Settings > Starling Integration — Example of SPS joined 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: Joined

Joined to Starling

This node is joined to Starling Services

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

Product Safeguard
Name

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

One Identity Starling integration

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

If you are using a Starling Two-Factor Authentication 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.

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

C

Cadence

Font that contains standard icons used in the user interfaces for various 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, usefull information.

A

authentication

 ['credential stores'] 35

C

certificate-mapping 35

certificates

 ['mapping'] 35

connection permissions

 ['querying permissions'] 43

credential stores 35

 ['local'] 32

H

HTTPS proxy 44

K

keymapping 35

L

limit concurrent connections 43

P

password 44

plugin 36

plugins 36

policies

 ['usermapping'] 30

port 44

proxy server 44

R

rate limiting 43

S

server-side authentication

 ['credential stores'] 35

T

throttle 43

U

user permissions

 ['connections'] 43

 ['user memberships'] 43

usermapping policies 30

username 44