One Identity Safeguard Remote Access
1.0

Administration 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.

SRA Administration Guide
Updated - 02 December 2021, 07:28
Version - 1.0
## Contents

**Introduction** ................................................................. 5

**Prerequisites** ................................................................. 6

**Limitations** ................................................................. 7

**Getting started** ............................................................ 8

Creating and signing in to a One Identity Starling account .................. 8

Creating a new organization ................................................ 8

Signing in to One Identity Starling ....................................... 10

Starting the One Identity Safeguard Remote Access trial ................. 11

Configure One Identity Safeguard for Privileged Sessions .................. 11

Configuring Usermapping policy ......................................... 12

Configuring a Credential store ........................................... 13

Upload Authentication and Authorization plugin .......................... 14

Configuring Authentication and Authorization plugin .................. 17

Configuring a connection policy ........................................ 17

HTTPS proxy ...................................................................... 22

Joining SPS to Starling ....................................................... 22

Enabling One Identity Safeguard Remote Access .......................... 23

**Administrator-side use cases** ............................................ 25

Administrator web interface location ..................................... 25

Adding a new connection to an existing target server .................... 25

Configuring the maximum RDP image resolution ........................ 27

Adding Azure Active Directory users directly ............................ 27

Granting connection access to AAD users ................................ 29

Enabling role-based access control ..................................... 31

Cloning connections ................................................................ 32

Deleting a connection ......................................................... 35

Inviting a One Identity Starling Collaborator ............................. 35

**User-side use cases** .......................................................... 37

User web interface location .................................................. 37

Connecting to the target server ............................................ 37
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session window</td>
<td>38</td>
</tr>
<tr>
<td>User Preferences tab</td>
<td>40</td>
</tr>
<tr>
<td>Appendix</td>
<td>42</td>
</tr>
<tr>
<td>About us</td>
<td>43</td>
</tr>
<tr>
<td>Contacting us</td>
<td>43</td>
</tr>
<tr>
<td>Technical support resources</td>
<td>43</td>
</tr>
<tr>
<td>Glossary</td>
<td>44</td>
</tr>
<tr>
<td>Index</td>
<td>46</td>
</tr>
</tbody>
</table>
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
To use One Identity Safeguard Remote Access (SRA), you must meet the following prerequisites:

- One Identity Safeguard for Privileged Sessions (SPS) version 6.9.0 or later is installed. Basic network configuration is completed, and the web administrative interface is available.
- One Identity Safeguard for Privileged Sessions (SPS) version 6.11.0 or later is installed, if SRA is intended to be used in a SPS cluster environment.
- A SPS Authentication and Authorization (AA) plugin is selected. For more information, see Using plugins.
- **Administrator** role under the SRA product in One Identity Starling.
Limitations

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

Security-related limitations:

- The end-user is not required to periodically re-authenticate to a running session. Once the 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.
- Only SSH and RDP protocols are fully supported, VNC and Telnet are only supported on a best effort basis.
- No RDP gateway is supported, SRA itself acts as the gateway.
- No RDP remote application or SCP over SSH 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 unjoined from One Identity Starling, then the related target connections remain visible on SRA.
- No Copy & Paste support in terminal sessions.
- The server-side resolution in terminal sessions cannot be changed.
- Inband target servers provided by the end user are currently not supported, only preset inband targets.
- Some browser keyword shortcuts are not forwarded to the terminal session, such as Ctrl-T, Ctrl-Shift-N.
- For Apple users, copy-pasting text in an active remote session with Cmd+C and Cmd+V keyboard shortcuts does not work. Use \(\text{Copy to clipboard}\) and \(\text{Paste}\) on the session window’s control panel to copy-paste text to/from the server.
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).

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**.
     4. **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.
     5. 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 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/](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](image)

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

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*
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 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*

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 and Using credential stores for server-side authentication 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**

  ![Download the first .zip file.](image)

  **SHA256 checksum:**
  
  8c28ac33b73f77fd82ef53e6e876d592f2861b32c63c6b5f336d5a35e6ddc995955d6f5f0b03

  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 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 Upload plugin.

Expected outcome: The plugin that you have uploaded is displayed:
Figure 7: Uploading the plugin

For more information on the HTTPS proxy setting, refer to the One Identity Safeguard for Privileged Sessions Administration Guide or part of it in Using plugins 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

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.
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

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).

1. **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

and **linux_servers** became the group containing one connection towards the 192.168.122.1 target.
2. **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 cloud 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.

3. **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.

4. **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.
5. **Policies**

Use the configuration for AA plugin (Configure Authentication and Authorization plugin), credential store (Credential store) and usermapping policy (User mapping 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**

For more information on the HTTPS proxy setting, refer to the One Identity Safeguard for Privileged Sessions Administration Guide or part of it in Configuring connections 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, refer to the One Identity Safeguard for Privileged Sessions Administration Guide, or to the relevant part of it in HTTPS proxy 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 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. |
For more information on the HTTPS proxy setting, refer to the One Identity Safeguard for Privileged Sessions Administration Guide, or the relevant part of it in Joining SPS to One Identity Starling 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**

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 (which is the target server itself)
- and an account (which is 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.
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

2. The Add new user to target server side sheet is split into two sections as connections comprise of assets and accounts. For Asset configuration:
   a. Specify the address of the target server that you want to access,
   b. Specify the access protocol of the new connection (for example, SSH, RDP or TELNET),
   c. Select a policy for this connection. To configure a policy in One Identity Safeguard for Privileged Sessions (SPS), navigate to Policies.

3. For Account configuration, specify a username and optionally a domain name to log in to this asset.

4. Click Create.
Configuring the maximum RDP image resolution

Configuring the RDP image resolution correctly results in a better stream quality.

| NOTE: A higher RDP image resolution results in higher network traffic load.

To configure the maximum RDP image resolution

1. Click the (Settings) and select Safeguard Remote Access Settings.
2. Find Select maximum image resolution for RDP.

3. Select the preferred image resolution.
   The default value is 1024x768.

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 AAD 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 AAD 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 AAD.

There is a user with Administrator role in that AAD. The Administrator must consent to One Identity Starling having read-only access to AAD, specifically to:

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

**Figure 17: Allow One Identity Starling to have access to your Azure Active Directory user groups**

---

**To add Azure Active Directory users directly**

1. Log into One Identity Starling ([https://account.cloud.oneidentity.com/](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 18: 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 19: Connection tile > Role assignment > Add new group — Finding your groups**
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.

**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:

1. Click (Settings) and select Safeguard Remote Access Settings.
2. Find Enable role-based access control (RBAC).
3. Slide the toggle to enable RBAC.

**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**.
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**.
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.

4. Click Delete.

Inviting a One Identity Starling Collaborator

Inviting a One Identity Starling collaborator makes it possible for multiple people to work simultaneously on a project.

**NOTE:** There are two ways of giving access to connections:

- Inviting collaborators who have One Identity Starling accounts.
- Adding Azure Active Directory (AAD) groups directly.
When you invite One Identity Starling collaborators, you cannot limit the accessibility to connections in One Identity Safeguard Remote Access (SRA). The role-based access control functionality of SRA is available only when AAD groups are added directly.

**To invite a One Identity Starling Collaborator with the User role**

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

   **Figure 24: Collaborators > Invite Collaborator - Inviting a One Identity Starling Collaborator**

3. Enter the **First Name**, **Last Name**, and **Email** of the collaborator.

   Below the **Invite Collaborator** button, you can view the list of all collaborators invited to the project, along with their **Status** and **Roles** too.
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 25: Connecting to the target server**

![Connecting to the target server](image)

**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 twice to display the full view.

- ![Minimize control panel](image)
  - (Minimize control panel)
  - Open up or minimize the control panel on the left side.

- ![Copy to clipboard](image)
  - (Copy to clipboard)

- ![Paste](image)
  - (Paste)

- ![Enter fullscreen mode](image)
  - (Enter fullscreen mode)
To exit the 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:

<table>
<thead>
<tr>
<th></th>
<th>Windows</th>
<th>Linux</th>
<th>Apple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+C</td>
<td>Ctrl+C</td>
<td>Ctrl+C</td>
<td>Ctrl+Shift+C</td>
</tr>
<tr>
<td>Ctrl+V</td>
<td>Ctrl+V</td>
<td>Ctrl+V</td>
<td>Ctrl+Shift+V</td>
</tr>
<tr>
<td>Ctrl+Shift+C</td>
<td>Ctrl+Shift+C</td>
<td>Ctrl+Shift+V</td>
<td></td>
</tr>
<tr>
<td>Ctrl+Shift+V</td>
<td>Ctrl+Shift+V</td>
<td>Ctrl+Shift+V</td>
<td></td>
</tr>
</tbody>
</table>

**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 10000 characters.

Use the copy-paste functionality of the control panel to copy-paste text to/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).
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.
   - The default value is 1024x768.
   - The setting can be applied only to the current browser.
Figure 27: Setting the default RDP image resolution

Select default RDP image resolution
This setting will only be applied to the current browser.
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.
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](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/](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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product
Glossary

C

Cadence
[[[Undefined variable TemplateGuideVariables.OneIdentityNameShort]]] font that contains standard icons used in the user interfaces for various [[[Undefined variable TemplateGuideVariables.OneIdentityNameShort]]] 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

Tip
Additional, useful information.