



leostream

Remote Desktop Access Platform

Integrating with SAML-Based Identity Providers

Supporting Multi-factor Authentication for your Leostream Environment

Version 202x
May 2023

Contacting Leostream

Leostream Corporation
77 Sleeper St.
PMB 02-123
Boston, MA 02210
USA

<http://www.leostream.com>
Telephone: +1 781 890 2019

To submit an enhancement request, email features@leostream.com.

To request product information or inquire about our future directions, email sales@leostream.com.

Copyright

© Copyright 2002-2023 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

Trademarks

The following are trademarks of Leostream Corporation.

Leostream™

The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

Microsoft, Active Directory, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. The Duo logo is a registered trademark of Duo Security, Inc. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

Leostream software is protected by U.S. Patent 8,417,796.

Contents

CONTENTS	3
OVERVIEW	4
DETERMINING YOUR LEOSTREAM SINGLE SIGN-ON URL	4
PREPARING YOUR IDENTITY PROVIDER	5
ADDING YOUR SAML IDP TO LEOSTREAM	5
GENERATING SERVICE PROVIDER XML FOR YOUR LEOSTREAM ENVIRONMENT	7
ASSIGNING POLICIES FOR SAML LOGINS	7
LOGGING IN TO THE ADMINISTRATOR WEB INTERFACE	9
ENABLING USERNAME AND PASSWORD LOGINS	9
SPECIFYING A SIGN OUT URL	10
USING LOCATIONS TO CONTROL ACCESS	11
EXAMPLE CONFIGURATION: USING LEOSTREAM WITH OKTA	14
EXAMPLE: USING LEOSTREAM WITH GOOGLE ACCOUNTS	18
STEP 1: CREATING A CUSTOM ATTRIBUTE FOR POLICY ASSIGNMENT	18
STEP 2: SETTING CUSTOM ATTRIBUTE VALUES FOR USERS	19
STEP 3: CREATING A CUSTOM SAML APP	19
STEP 4: ADDING THE GOOGLE AUTHENTICATION SERVER TO LEOSTREAM	21
STEP 5: ASSIGNING POLICIES BASED ON CUSTOM GOOGLE ATTRIBUTES	22
EXAMPLE: USING LEOSTREAM WITH MICROSOFT ADFS	23
STEP 1: OBTAIN THE ADFS FEDERATION METADATA	23
STEP 2: CREATE A SAML AUTHENTICATION SERVER FOR ADFS	23
STEP 3: CREATE A RELYING PARTY TRUST FOR LEOSTREAM	24
EXAMPLE: SAML-LOGINS WITH PCOIP CONNECTIONS	31
EXAMPLE: USING MULTIPLE SAML SERVERS	34
STEP 1: DEFINING SAML TENANTS	34
STEP 2: DEFINING SAML SERVERS PER TENANT	36
EXTRA: SORTING DESKTOPS INTO TENANTS	37

Overview

Leostream 9 allows you to leverage SAML-based Identity Providers (IdP) to provide single sign-on to the Leostream web client with multi-factor authentication. You can integrate Leostream with any authentication service, such as Azure AD, Okta, Duo, and Ping Identity, that acts as a SAML 2.0 Identity Provider.

After enabling Leostream to work with your IdP, end users authenticate against the Identity Provider, which subsequently uses the SAML protocol to provide single sign-on for the user into your Leostream environment. In this scenario, the Leostream Connection Broker never processes the user's credentials and knows only the information provided about the user by the SAML IdP.

 SAML logins are currently supported only for user's logging in using the Leostream Web client. Leostream Connect, thin client, and zero client logins do not support SAML-based authentication. Leostream Web client logins can launch the following display protocols.

- Microsoft RDP
- NoMachine
- NICE DCV
- Scyld
- VNC
- HP ZCentral Remote Boost (RGS)
- Mechdyne TGX
- Teradici PCoIP to desktops running the Cloud Access Software

When enabled, all domain users should authenticate against the IdP in order to gain access to your Leostream environment. You can optionally allow users to bypass SAML authentication, as described in [**Enabling Username and Password Logins**](#).

Determining your Leostream Single Sign-On URL

You typically require two key pieces of information to register Leostream with your SAML-based IdP.

1. Your Leostream Entity ID – You specify this value in the **SAML EntityID** edit field when you create your SAML-based Authentication server in Leostream. This value should be unique across all your Leostream environments and the SAML applications in your IdP.
2. Your Leostream single sign-on URL – This is the endpoint where your SAML IdP sends the SAML assertion to the log user into Leostream.

The Leostream single sign-on URL is the URL that your SAML-based Identity Provider users to pass the SAML assertion to the Leostream Connection Broker after the user successfully authenticates. Generally, the URL takes the following form:

```
https://leostream-login-address/saml
```

Where *leostream-login-address* is the address end users go to to access your Leostream environment. This could be any of the following.

- For a standalone Connection Broker, the IP address or hostname of that Connection Broker
- For a Connection Broker cluster, the VIP of the cluster, which may be the IP address or FQDN of the load balancer in front of the cluster.
- For Leostream logins forwarded through the Leostream Gateway, the IP address or FQDN of the Leostream Gateway that is forwarding the Leostream login traffic, or the IP address or FQDN of the load balancer in front of the Leostream Gateway.

In some cases, your Identity Provider requires this information in XML format, which you can generate in Leostream after you create your SAML Authentication Server (see [Generating Service Provider XML for your Leostream Environment](#)).

Preparing Your Identity Provider

When using a SAML IdP as the authentication method for your Leostream environment, Leostream assigns policies to users based on the attributes contained in the SAML assertion returned to Leostream by your IdP. Before integrating your IdP with Leostream, ensure that you configure your IdP to return appropriate user attributes.

Then, obtain the following information from your SAML IdP:

- The IdP login URL
- The IdP Federation XML Metadata

How you setup your identity provider to support Leostream as a SAML service provide and obtain the login URL and metadata depends on which IdP you use. See [Example Configuration: Using Leostream with Okta](#) or [Example: Using Leostream with Google Accounts](#) for examples.

Adding Your SAML IdP to Leostream

In order to register your Leostream environment with your SAML IdP you must create an authentication server for your IdP in your Connection Broker, as follows.

1. Go to the > **Setup > Authentication Servers** page.
2. Click the **Add Authentication Server** link.
3. Select **SAML** from the **Type** drop-down menu.

 You can add one SAML IdP to your Connection Broker for each tenant defined in your Leostream environment. If you need to define multiple SAML tenants, contact sales@leostream.com to enable multi-tenancy in your Leostream environment.

4. Enter a descriptive name in the **Authentication Server Name** field.
5. In the **SAML EntityID** edit field, enter the unique Entity ID to use for your Connection Broker in your SAML-based Identity Provider.
6. The **SAML Attribute Mappings** section allows you to relate data returned in the SAML assertion to fields used to define user records in the Connection Broker. Currently, you can map values for the user's name (shown in the **Name** column on the > **Resources** > **Users** page) and email address (shown in the **Email** column on the > **Resources** > **Users** page).

Use the {SAML} dynamic tag to specify attributes returned in the SAML assertion. As a couple examples:

- For **Name**, enter {SAML:LastName}, {SAML:FirstName} to display the user's last name and first name separated by a comma. The attributes are case sensitive so LastName and FirstName must be returned as attributes in the SAML assertion
 - For **Email address**, enter {SAML:http://schemas.xmlsoap.org/claims/email} if an attribute named email is returned in the SAML assertion as a URI reference.
7. In the **Connection Settings** section, shown in the following figure, enter the **Identity Provider login URL** and the **Identity Provider XML Metadata** obtained from your identity provider.



Connection Settings

Identity Provider login URL

All Connection Broker login traffic will be redirected to this address

Enable user logins without SAML at "https://10.110.37.22/login"
Connection Broker administrators can always log in at "https://10.110.37.22/admin"

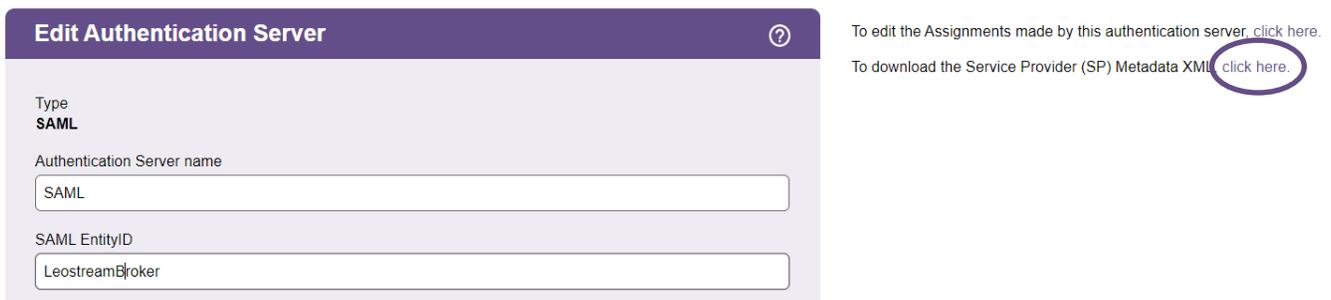
Identity Provider XML metadata

8. By default, after you created a SAML-based authentication server, the Connection Broker redirects all users to the Identity Provider's login URL when the user visits the Connection Broker login page. To allow users to bypass the SAML-based authentication server, select the **Enable user logins without SAML** check box. See [Enabling Username and Password Logins](#) for more information.
9. Click **Save** to save the form.

Generating Service Provider XML for your Leostream Environment

You can generate the Service Provider (SP) XML for your Leostream environment after you save your SAML-based authentication server (see [Preparing Leostream to Work with Your SAML IdP](#)) as follows.

1. Go to the **> Setup > Authentication Servers** page.
2. Click the **Edit** link for your SAML authentication server.
3. Click the link to the right of the **Edit Authentication Server** form to download the SP XML needed to setup your IdP, for example:



The screenshot shows the 'Edit Authentication Server' interface. The form contains the following fields:

- Type: **SAML**
- Authentication Server name:
- SAML EntityID:

To the right of the form, there are two links:

- To edit the Assignments made by this authentication server, [click here.](#)
- To download the Service Provider (SP) Metadata XML, [click here.](#) (This link is circled in red in the image.)

The SP XML downloads to a file named `leostream.xml`. This file contains two important parameters

- `entityID` = The value if you entered in the **SAML EntityID** edit field when you created your SAML-based Authentication server the Leostream. This should be a unique value when compared to any other service providers registered with your identity provider.
- `Location` = `https://<login_ip>/saml` – Where `<login_ip>` is the IP address of your Connection Broker. In clustered environments, edit this value so it is the VIP of your Leostream cluster. If you are using a Leostream Gateway to forward login traffic to your Connection Broker, enter the IP address or hostname of the Leostream Gateway or the load balancer for your Leostream Gateways, if applicable. See [Determining your Leostream Single Sign-on URL](#) for complete instructions.

Follow the instructions provided by your IdP to register your Leostream environment using the SP XML.

Assigning Policies for SAML Logins

When you have an active SAML authentication server configured in your Leostream environment, policies are assigned to users based on the list of attributes returned to Leostream by your SAML IdP upon successful authentication.

To assign a policy to a user, Leostream matches those attributes against the assignment rules defined on the **> Configuration > Assignments** page for your SAML IdP. You configure your assignment rules, as follows.

1. Go to the > **Configuration > Assignments** page in your Leostream Connection Broker.
2. Click **Edit** for your SAML IdP.
3. Enter the specific attribute Leostream to use for policy assignments into the **Attribute** edit field. Your available attributes depend on the SAML assertion returned by your IdP.
4. Select the appropriate **Conditional**, typically **Contains**.
5. In the **Attribute Value** field, map values of the attribute to the appropriate roles and policies.

In the following figure, the assertion returns attributes as URIs so the **Attribute** field contains a full URL. If the attributes are returned as text values, the **Attribute** field in this example would be **Group** instead of **http://schemas.xmlsoap.org/claim/Group**.

Edit Assignments for Authentication Server "SAML"

Assigning User Role and Policy
 In this section, you can set up rules to assign Users to Roles and Policies based on their SAML attributes. Optionally, use the Order column to re-order the rows.

Attribute: Conditional:

The Conditional setting controls how the user's SAML Attribute and entered Attribute Value must match in order for the user to be assigned that role and policy.

Order	Attribute Value	Client Location	User Role	User Policy
1	<input type="text" value="Development"/>	<input type="text" value="Leostream Connect"/>	<input type="text" value="User"/>	<input type="text" value="Default"/>
2	<input type="text" value="Sales"/>	<input type="text" value="Web Browsers"/>	<input type="text" value="User"/>	<input type="text" value="Default"/>
3	<input type="text"/>	<input type="text" value="All"/>	<input type="text" value="User"/>	<input type="text" value="Default"/>

[Add rows]

Default Role:

Default Policy:

Users will be assigned the default role and policy if they don't match an assignment rule

6. Select the appropriate policy for the different groups of users from the **User Policy** drop-down menus.
7. To block logins for any users that successfully authenticate with the SAML IdP but who should not have access to your Leostream environment, select **<None – prevent user login>** from the **Default Policy** drop-down menu below the assignments table, as shown in the previous figure.

Logging in to the Administrator Web Interface

When you have an active SAML authentication server configured in your Leostream environment, the following Connection Broker URLs automatically redirect all users to your IdP login page.

- `https://leostream-address`
- `https://leostream-address/index.pl`

Where `leostream-address` is the IP address or fully qualified host name of your Leostream environment, which may be your Leostream Gateway or load balancer address.

To log into the administrator interface as the default `admin` user or as a domain user with an Administrator role, go to:

```
https://leostream-address/admin
```

Users who do not have Role access to the Administrator Web interface receive an `Invalid username or password` error when attempting to log into this URL. If you have users who should be able to log in with their domain credentials, enable the end-user login URL, as described in the following section.

Enabling Username and Password Logins

By default, when a SAML-based authentication server is defined in Leostream, all end-user logins must authenticate with your Identity Provider to gain access to your Leostream environment. If you have local users or domain users who are allowed to bypass your Identity Provider and use their username and password to log into Leostream, you can enable the end-user URL, as follows.

1. Go to the **> Setup > Authentication Servers** page.
2. Edit your SAML authentication server.
3. Select the **Enable login without SAML** checkbox.

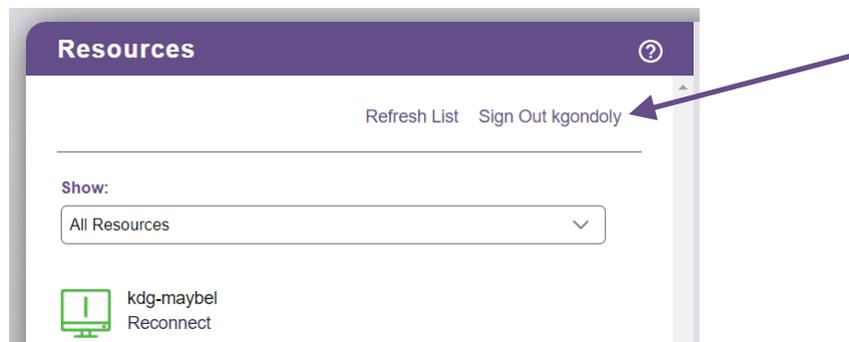
The prompt uses your current Connection Broker address as an example of the end-user URL. The actual address in your end-user URL depends on your Leostream architecture, and may be the address of your Leostream Gateway or load balancer. The end-user URL is the user-facing hostname or IP address of your Leostream environment appended with `/login`.

4. Click **Save**.

You can use Locations to restrict which Domain users are allowed to log in using their username and password, as described in [Using Locations to Control Access](#).

Specifying a Sign Out URL

The Leostream Web client contains a **Sign Out** link, shown in the following figure.

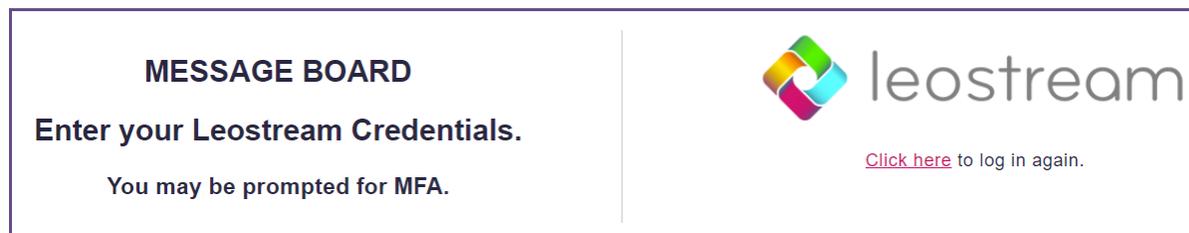


The **Sign Out** link signs the user out of their Leostream session.



The **Sign Out** link does not perform SAML Single Logout.

By default, the user is redirected to a Sign Out page similar to that shown in the following figure.



You can use the **URL redirect on user logout** field on the **> System > Settings** page to redirect the user to your sign-out page of choice. For example, the following figure redirects the user to <https://www.leostream.com>.

 A screenshot of the "Web Browser Configuration" settings page. It contains several configuration options:

- "Display Connection Broker logo and favicon:" with a dropdown menu set to "Leostream". Below it is a note: "To select Custom, you must first Upload Logos and Favicons as 'custom_logo.png', 'custom_logo.gif', or 'custom_logo.jpg', and 'favicon.ico'".
- "Web client skin:" with a dropdown menu set to "<Default>".
- "Additional text for left side of sign-in form" with a text area containing HTML code:


```
<center><h2>Enter your Leostream Credentials.</h2>
      <h3>You may be prompted for MFA.</h3></center>
```

 Below the text area is a note: "HTML may be used."
- "URL redirect on user logout" with a text input field containing "https://www.leostream.com".
- A checkbox labeled "Show Message Board on Web Client" which is checked.

The URL must include the `http://` or `https://` prefix to send the user to a page outside of your Leostream environment. Without the HTTP prefix, the URL takes the form:

```
http://leostream-address/URL-to-redirect
```

Where *leostream-address* is the end-user facing address of your Leostream environment and *URL-to-redirect* is the text entered in the **URL redirect on user logout** field. This may be useful if you uploaded a custom sign out page into your Leostream Connection Broker machine.

Using Locations to Control Access

Users can log into Leostream from a variety of client types, including Web browsers, thin clients, zero clients, and Leostream Connect software clients. SAML-based authentication is available only for Web browser logins.

For other client types, you can use Leostream locations and assignment rules to determine if users are allowed to log in. You can also use Locations to allow and prevent username and password logins for groups of users if you have enabled the end-user URL (see **Enabling Username and Password Logins**).

Example 1: Blocking Domain Users from Logging into the End-User URL

If you have a mixture of on-premises and remote users, you may want to require remote users to log in using your SAML-based Identity Provider while allowing on-premises users to log in with their domain credentials. To do this:

- 1) Create a location that includes your on-premises subnets, for example, the following figure creates a location for all client devices on the 172 network.

?
Create Location

Name

Subset of location

Attribute Selection

Client attribute	Conditional	Value
<input type="text" value="IP address"/>	<input type="text" value="matches (CIDR notation)"/>	<input type="text" value="172.0.0.0/8"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="[Add rows]"/>		

The Clients must match any of the attribute rules (OR)
 The Clients must match all of the attribute rules (AND)

- 2) Set the Assignments table for your on-premises authentication server to assign a Role and Policy for this location.
- 3) Deny access otherwise, by setting the **Default Policy** to **<None - prevent User Login>**, for example:

Assigning User Role and Policy
In this section, you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally, use the Order column to re-order the rows.

Order	Group	Client Location	MFA Provider	User Role	User Policy
1	<input type="text" value="Administrators"/>	+ <input type="text" value="All"/>	+ <input type="text" value="<Not required>"/>	→ <input type="text" value="Administrative"/>	& <input type="text" value="<No policy>"/>
2	<input type="text" value="Domain Users"/>	+ <input type="text" value="On-Premises"/>	+ <input type="text" value="<Not required>"/>	→ <input type="text" value="User"/>	& <input type="text" value="Default"/>
3	<input type="text"/>	+ <input type="text" value="All"/>	+ <input type="text" value="<Not required>"/>	→ <input type="text" value="User"/>	& <input type="text" value="Default"/>
<input type="text" value="[Add rows]"/>					

Default MFA Provider

Default Role

Default Policy

In the figure above, all domain Administrators are allowed to log in with their Domain credentials and access the Administrator Web interface. Domain users who log in from an on-premises client are allowed to log into the Web client to access their desktops. All other users are blocked from logging in.

Example 2: Blocking end-user logins from non-Web browser clients types

SAML-based authentication is supported only for users logging in from the Leostream Web client. Other client types, such as Leostream Connect or PCoIP clients allow username and password authentication, with optional MFA using a RADIUS server, unless you specifically block those logins. To block user logins from other client types, you can create a Leostream Location for all non-Web browser clients, for example:

?
Create Location

Name

Subset of location

Attribute Selection

Client attribute	Conditional	Value
<input type="text" value="Device type"/>	<input type="text" value="is not equal to"/>	<input type="text" value="Web Browser"/>

Use the **Assignments** table for you on-premises authentication server to assign a policy to users logging in from this location, allow Administrator access from the Web browser location, and block all other access, for example:

?
Edit Assignments for Authentication Server "Leodev"

Domain name
leodev.net

Assigning User Role and Policy
 In this section, you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally, use the Order column to re-order the rows.

Order	Group	+	Client Location	+	MFA Provider	→	User Role	&	User Policy
1	<input type="text" value="Administrators"/>		<input type="text" value="All"/>		<input type="text" value="<Not required>"/>		<input type="text" value="Administrator"/>		<input type="text" value="<No policy>"/>
2	<input type="text" value="Domain Users"/>		<input type="text" value="Non Web browsers"/>		<input type="text" value="<Not required>"/>		<input type="text" value="User"/>		<input type="text" value="<No policy>"/>
3	<input type="text" value="Domain Users"/>		<input type="text" value="On-Premises Client"/>		<input type="text" value="<Not required>"/>		<input type="text" value="User"/>		<input type="text" value="Default"/>

Example Configuration: Using Leostream with Okta

To use Okta as the authentication portal for your Leostream environment, you add Leostream as a SAML 2.0 application in your Okta account then create a SAML Authentication Server in your Connection Broker. The following procedure describes how to add the SAML 2.0 application in your Okta account

1. Log into your Okta Admin portal.
2. From the top-level **Applications** menu, select **Applications**.
3. In the **Applications** page, click the **Create App integration** button.
4. In the **Create a new app integration** page,
 - a. Select **SAML 2.0** in the set of radio buttons.
 - b. Click **Next**.
5. In the first page of the **Create SAML Integration** form:
 - a. Provide a descriptive name in the **App name** edit field.
 - b. Optionally set the logo and app visibility.
 - c. Click **Next**.
6. In the **SAML Settings** on the second page of the **Create SAML Integration** form, complete the following two fields. Additional fields can be configured or left with their default values, depending on your requirements.
 - a. The **Single sign on URL** for your Leostream environment is the IP address or hostname that you currently use to log into your Leostream environment, followed by `/saml`. For example:
 - If you have a single Connection Broker with a DNS name of `vdi-portal.mycompany.net`, the **Single sign on URL** is `https://vdi-portal.mycompany.net/saml`.
 - If you have a cluster of Connection Brokers behind a load balancer, the **Single sign on URL** is the load balancer IP address or FQDN.
 - If you use a Leostream Gateway to forward login traffic to your Connection Broker, the **Single sign on URL** is the Leostream Gateway address or the address of the load balancer used with multiple Leostream Gateways.
 - b. In the **Audience URI (SP Entity ID)** field, enter a text value that you will use as the Entity ID when defining the SAML authentication server in your Connection Broker, for example `LeostreamBroker`.

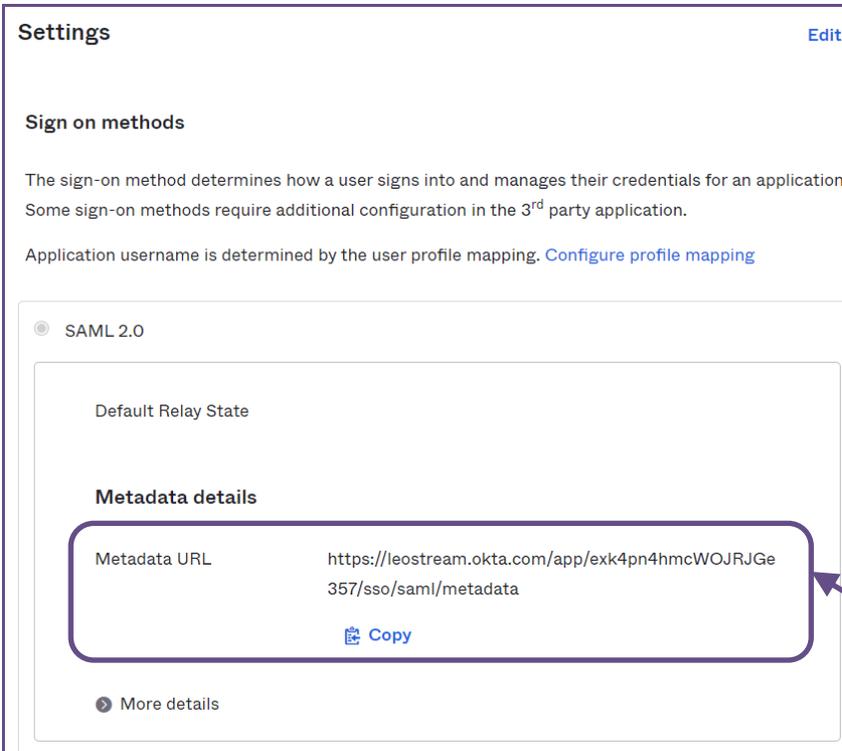
7. In the **Attribute Statements** below the **SAML Settings**, enter the user attributes that Okta sends to Leostream in the SAML assertion that follows a successful Okta login. The user and group attributes represent the values you can use to assign policies in Leostream. The following table describes an example that sends the user's login name, email address, and first and last names.

Name	Name format	Value
login	Unspecified	user.login
email	Unspecified	user.email
firstname	Unspecified	user.firstName
lastname	Unspecified	user.lastName

8. Use the **Group Attribute Statements** section to send the user's Okta groups to Leostream, to use for policy assignments. To send a list of all the groups the user is member of, enter the following values:
- Name:** Groups
 - Name format:** Unspecified
 - Filter:** Matches regex
 - Filter text:** .*
9. Click **Next** in this page of the **Create SAML Integration** form
10. In the final page of the **Create SAML Integration** form, select the **I'm an Okta customer adding an internal app** radio button and click **Finish**.

After creating your application, assign the appropriate users to this application in Okta. Only assigned users can log into your Leostream environment.

After assigning users to your new Leostream application, go to the Metadata URL to obtain the information you need to add the SAML Authentication Server to your Leostream Connection Broker. You can find the **Metadata URL** on the **Sign On** tab of your SAML 2.0 application, indicated in the following figure.



Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Metadata details

Metadata URL	https://leostream.okta.com/app/exk4pn4hmcWOJRJGe357/sso/saml/metadata
--------------	---

[Copy](#)

More details

Clicking the link opens the XML metadata in a new Web Browser tab. Use the browser's option to view the page source or copy the contents of this page to a text editor so you can copy the XML metadata without any formatting and without the initial text line indicating the XML file does not contain style information.

After obtaining the XML metadata, log into your Connection Broker Administrator Web interface to add the SAML Authentication Server, as follows.

1. In your Connection Broker Administrator Web interface, go to the **> Setup > Authentication Servers** page.
2. Click the **Add Authentication Server** link at the top of the page.
3. In the **Add Authentication Server** form, select **SAML** from the **Type** drop-down menu.
4. Enter a descriptive name in the **Authentication Server name** edit field.
5. For the **Identity Provider login URL**, enter the full URL to the single sign on service for your new SAML 2.0 application. You can find this URL by clicking the **View Setup Instructions** button on the **Sign On** tab of your SAML 2.0 application. Use the value specified for the **Identity Provider Single Sign-On URL**.
6. In the **Identity Provider XML metadata** field, paste the entire, unformatted XML metadata downloaded from your SAML 2.0 application in Okta.
7. Click **Save**.

After adding the Okta SAML Authentication Server to your Connection Broker, all user logins are redirected to Okta. To access your Connection Broker Administrator web page, you must add `/admin` to your Connection Broker login URL.

To assign policies to users based on their Okta group membership, go to the **> Configuration > Assignments** page in your Connection Broker and edit the assignments table associated with your Okta SAML authentication server.

For example, given the previous setup, to assign a policy to all the users in the Leostream group, the **Assignments** table is configured as follows and shown in the subsequent figure.

- **Attribute:** Groups
- **Conditional:** Contains
- **Attribute Value:** Leostream
- **User Policy:** Default

Edit Assignments for Authentication Server "Okta" ?

Assigning User Role and Policy
 In this section, you can set up rules to assign Users to Roles and Policies based on their SAML attributes. Optionally, use the Order column to re-order the rows.

Attribute: Conditional:

The Conditional setting controls how the user's SAML Attribute and entered Attribute Value must match in order for the user to be assigned that role and policy.

Order	Attribute Value	Client Location	User Role	User Policy
1	<input type="text" value="Leostream"/>	+ <input type="text" value="All"/>	→ <input type="text" value="User"/>	& <input type="text" value="Default"/>
2	<input type="text"/>	+ <input type="text" value="All"/>	→ <input type="text" value="User"/>	& <input type="text" value="Default"/>
3	<input type="text"/>	+ <input type="text" value="All"/>	→ <input type="text" value="User"/>	& <input type="text" value="Default"/>

Default Role:

Default Policy:

Users will be assigned the default role and policy if they don't match an assignment rule

Example: Using Leostream with Google Accounts

If your organization uses Google Workspace, you can authenticate users into your Leostream environment with their Google account by creating a custom SAML app for your Leostream environment. After the user authenticates with Google, your Leostream Connection Broker assigns policies to the users based on the attributes returned by Google.

You can leverage Google Groups to indicate which users are allowed to log into Leostream. However, you cannot return Google Group information in the SAML assertion sent to Leostream. Therefore, if you want to assign policies to groups of users, you must create a custom attribute and set that attribute value appropriate for each user.

Step 1: Creating a Custom Attribute for Policy Assignment

To create a custom attribute:

1. Log into your Google Admin console.
2. Go to **Users**.
3. At the top of **Users** list, click **More** and select **Manage custom attributes**.
4. Click **Add Custom Attribute** at the top-right.
5. In the **Add custom field** form, enter the **Category** and **Description** as desired.
6. In the **Custom fields** section:
 - a. Set the **Name** of the attribute to use in the **Assignments** table in Leostream
 - b. Select **Text** from the **Info type** drop-down menu.
 - c. Select **Visible to organization** from the **Visibility** drop-down menu.
 - d. Select **Multi-value** from the **No. of values** drop-down menu, for example:

Add custom fields

Category
Leostream Groups

Description
Group names for Leostream App SAML assertion

Custom fields

Name	Info type	Visibility	No. of val...	
LeostreamGroups	Text	Visible to ...	Multi-value	X
Name	Info type	Visibility	No. of val...	

CANCEL ADD

7. Click **Add**.

Step 2: Setting Custom Attribute Values for Users

After creating the custom attribute, set the attribute value appropriately for each user who logs into your Leostream environment.

1. Log into your Google Admin console.
2. Go to **Users**.
3. In the **Users** list, click the username to add to a Leostream group.
4. Expand the **User information** section.
5. Enter in every group that this user is a member of, for example:

Leostream Groups

LeostreamGroups

Editors

LeostreamGroups

Engineers

LeostreamGroups

CANCEL SAVE

6. Click **Save**.

Step 3: Creating a Custom SAML App

To connect your Leostream environment to your Google Workspace, create a custom SAML App on Google Workspace, as follows.

1. Log into your Google Admin console.
2. Go to **Apps > Web and mobile apps**.
3. At the top of **Apps** list, click **Add App** and select **Add custom SAML app**.
4. In the **App details** form,
 - a. Specify the **App name**. This name cannot be changed after you create the custom SAML app.
 - b. Optionally enter an **App icon**.
 - c. Click **Continue**.
5. On the form to configure SSO for SAML apps:
 - a. Download the IdP metadata
 - b. Copy the SSO URL, indicated in the following figure.

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

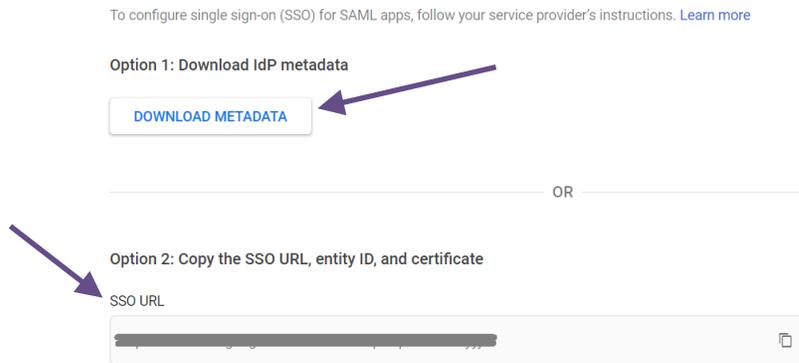
Option 1: Download IdP metadata

[DOWNLOAD METADATA](#)

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL



- c. Click **Continue**.
6. In the **Service provider details** form:
 - a. Enter the Leostream single sign-on URL in the **ACS URL** field. See **Determining your Leostream Single Sign-On URL** for more information on how to determine this URL.
 - b. Specify a unique **Entity ID**. Make note of this value as you will use it when creating the authentication server in your Leostream Connection Broker.
 - c. Select **Email** from the **Name ID format** field.
 - d. Select **Basic Information > Primary email** from the **Name ID** drop-down menu.
 - e. Click **Continue**.
 7. In the **Attributes** form, add all the attributes that Google should send to your Leostream Connection Broker in the SAML assertion.
 - a. In the **Google Directory attributes** column, select the attribute from the **Select field** drop-down menu. Your custom attributes are included at the bottom of this list. Ensure that you send your custom attribute for policy assignment, along with any other attributes you want associated with the user records in Leostream.
 - b. In the **App attributes** column, enter the parameter name to use in the SAML assertion. These are the attribute names you reference in the SAML authentication server in your Leostream environment, as described in the next section, for example:

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes		App attributes	
Basic Information > First name	▼ →	First Name	×
Basic Information > Last name	▼ →	Last Name	×
Basic Information > Primary email	▼ →	Email	×
Leostream Groups > LeostreamGroups	▼ →	LeostreamGroups	×

8. Click Finish.

Google may try to log you into your Leostream environment when you finish configuring the custom SAML app. This login fails until you complete the remainder of the setup procedure described in this example. Please continue through step 5 to finalize the integration of Google with your Leostream environment.

By default, the custom SAML application is off for all users. To allow access to the application for some or all of the users in your Google directory:

1. Log into your Google Admin console.
2. Go to **Apps > Web and mobile apps** page.
3. Select your new SAML application.
4. Expand the **User access** section of the page.
5. Select the scope of users to enable access and select **On** from the **Service status**.
6. Click **Save**.

Step 4: Adding the Google Authentication Server to Leostream

You add Google as a SAML-based authentication server in your Connection Broker, as follows.

1. Go to the **> Setup > Authentication Servers** page.
2. Click the **Add Authentication Server** link.
3. Select **SAML** from the **Type** drop-down menu.
4. Enter a descriptive name in the **Authentication Server Name** field.
5. In the **SAML EntityID** edit field, enter the Entity ID you specified for the custom SAML app in Google.

6. The **SAML Attribute Mappings** section allows you to relate data returned by Google in the SAML assertion to fields used to define the user records in the Connection Broker. Use the `{SAML}` dynamic tag to specify attributes returned in the SAML assertion, for this example
 1. For **Name**, enter `{SAML:Last Name}`, `{SAML:First Name}`
 2. For **Email address**, enter `{SAML:Email}`
7. In the **Connection Settings** section:
 1. Enter the **SSO URL** copied from your custom SAML app into the **Identity Provider login URL** field.
 2. Copy the content of the XML metadata file downloaded from your custom SAML app into the **Identity Provider XML Metadata** field.
8. Click **Save** to save the form

Step 5: Assigning Policies based on Custom Google Attributes

To assign policies to users based on the custom attributes you defined in your Google Workspace, go to the **> Configuration > Assignments** page in your Connection Broker and edit the assignments table associated with your Google authentication server.

For example, given the previous setup, to assign a policy to all the users in custom `LeostreamGroups`, the **Assignments** table is configured as shown in the subsequent figure.

Edit Assignments for Authentication Server "Google" ?

Assigning User Role and Policy
 In this section, you can set up rules to assign Users to Roles and Policies based on their SAML attributes. Optionally, use the Order column to re-order the rows.

Attribute: Conditional:

The Conditional setting controls how the user's SAML Attribute and entered Attribute Value must match in order for the user to be assigned that role and policy.

Order	Attribute Value		Client Location		User Role		User Policy
1	<input type="text" value="Development"/>	+	<input style="border: none; background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;" type="text" value="All"/>	→	<input style="border: none; background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;" type="text" value="User"/>	&	<input style="border: none; background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;" type="text" value="Default"/>
2	<input type="text"/>	+	<input style="border: none; background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;" type="text" value="All"/>	→	<input style="border: none; background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;" type="text" value="User"/>	&	<input style="border: none; background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;" type="text" value="Default"/>

Example: Using Leostream with Microsoft ADFS

The following procedure describes how to configure Leostream and Microsoft Active Directory Federation Services (ADFS) to work together using the Leostream support for the SAML protocol.

Please consult the appropriate Microsoft Knowledge Base article for information on setting up ADFS.

Step 1: Obtain the ADFS Federation Metadata

To create a SAML authentication server in Leostream for Microsoft ADFS, you must first reformat the ADFS Federation Metadata, as described in the following procedure.

1. Login into your Connection Broker machine console as the root user.
2. Navigate to the `/tmp` by executing the following command in a terminal.

```
cd /tmp
```

3. Execute the following command to download the Metadata XML file from ADFS.

```
wget https://<FQDN_ADFS>/FederationMetadata/2007-06/FederationMetadata.xml
```

Where `<FQDN_ADFS>` is the fully qualified domain name of your Microsoft ADFS server.

4. Execute the following command to format the Metadata XML.

```
xmllint --format /tmp/FederationMetadata.xml > /tmp/ADFS.xml
```

5. Execute the following command to output only the needed XML Parameters for SAML.

```
xsltproc adfs2md.xsl /tmp/ADFS.xml > IdP_SAML.xml
```

Please contact support@leostream.com to obtain the `adfs2md.xsl` file.

6. Copy the `IdP_SAML.xml` file from your Connection Broker to your local machine or some other location where it will be accessible from the Connection Broker Administrator Web interface.

Step 2: Create a SAML Authentication Server for ADFS

After you have the formatted Federation Metadata XML, you can create an authentication server in your Leostream Connection Broker that communications with ADFS using SAML, as follows.

1. Log into your Connection Broker Administrator Web interface.

2. Go to the > **Setup > Authentication Servers** page in your Connection Broker.
3. Click the **Add Authentication Server** link to add a new SAML Server.
4. In the **Add Authentication Server** form, select **SAML** from the **Type** drop-down menu.
5. Enter a name for your ADFS server in the **Authentication Server name** edit field.
6. In the **SAML EntityID** field, enter your preferred SAML Entity ID, for example **LeostreamBroker**.
7. In the **Identity Provider login URL** field, enter:

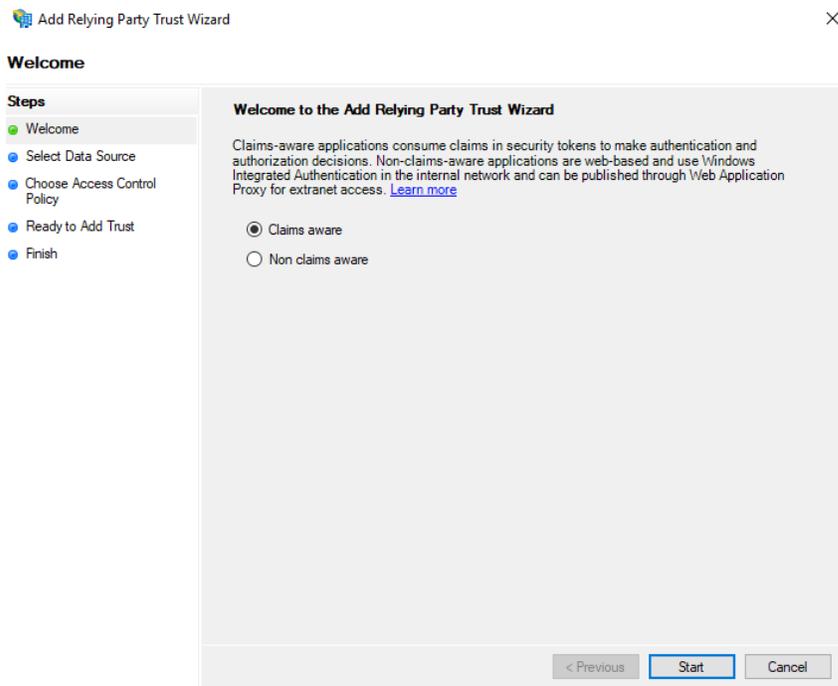
```
https://<FQDN_ADFS>/adfs/ls
```

Where *<FQDN_ADFS>* is the fully qualified domain name of your ADFS server.
8. Copy and paste the contents of the `IdP_SAML.xml` file into the **Identity Provider XML metadata** field.
9. Click **Save**.
10. After saving the form, click the **Edit** action associated with the new SAML authentication server.
11. Click the link at the top-right of the Authentication Servers page to download the Service Provider (SP) Metadata XML.

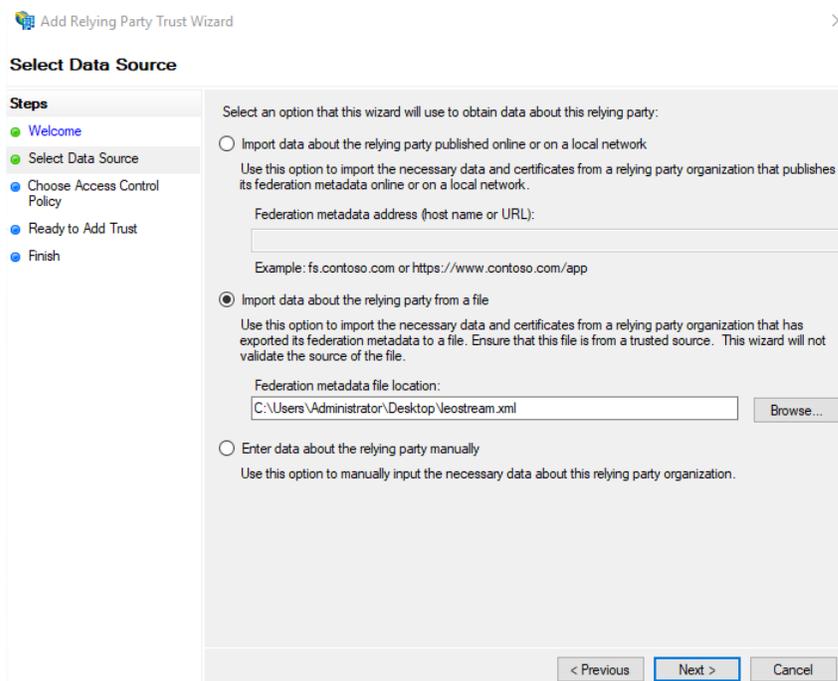
Step 3: Create a Relying Party Trust for Leostream

Next, configure your ADFS server to accept communications from your Leostream Connection Broker, by creating a Relying Party Trust

1. In your ADFS server, add a new Relying Party Trust.
2. In the **Add Relying Party Trust Wizard**, select the **Claims aware** option and click **Start**, as shown in the following figure.

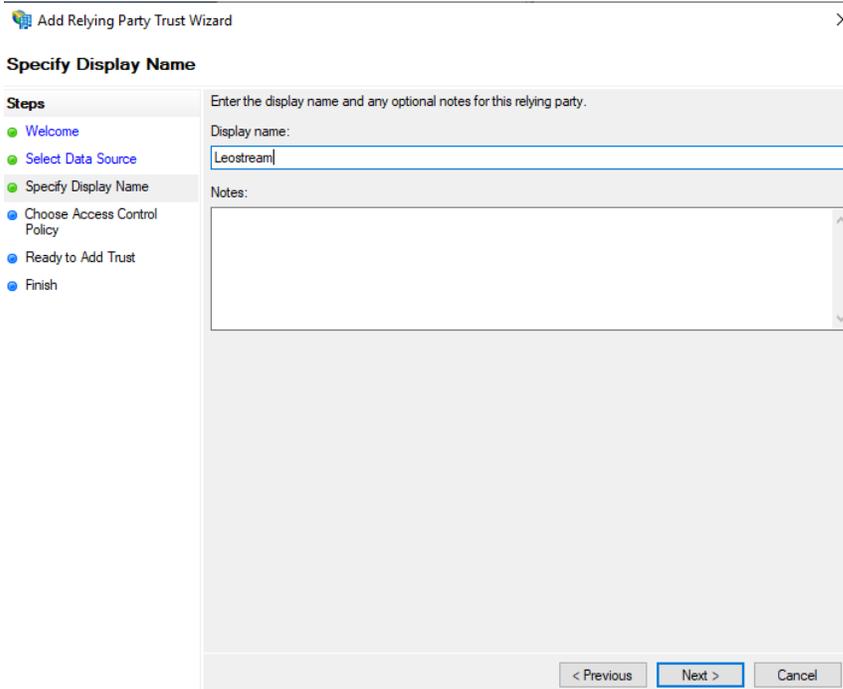


3. In the **Select Data Source** page, select the **Import data about the relying party from a file** option, as shown in the following figure.

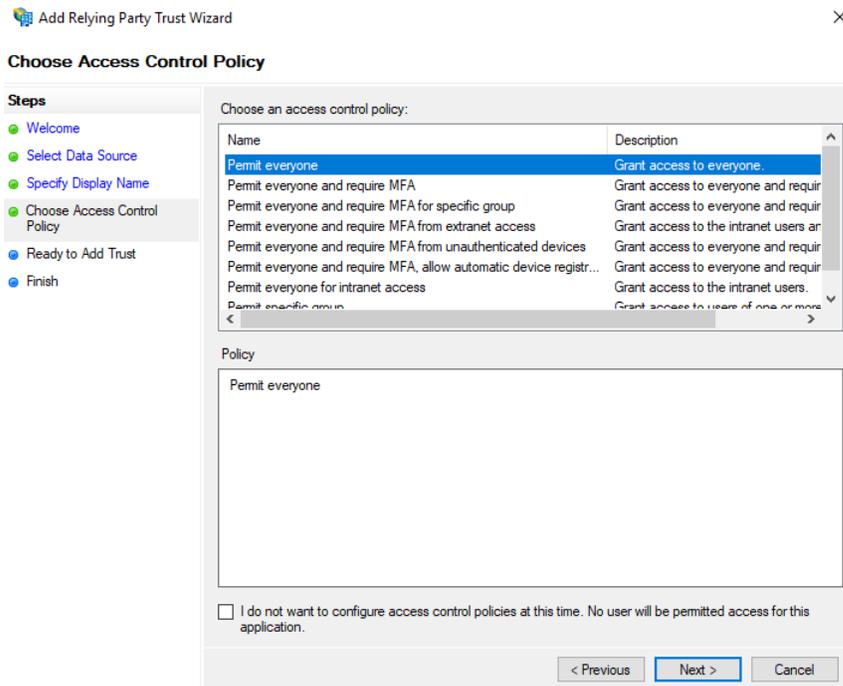


4. Click the **Browser** button to browser to and select the SP Metadata you downloaded in Step 2.
5. Click **Next**.

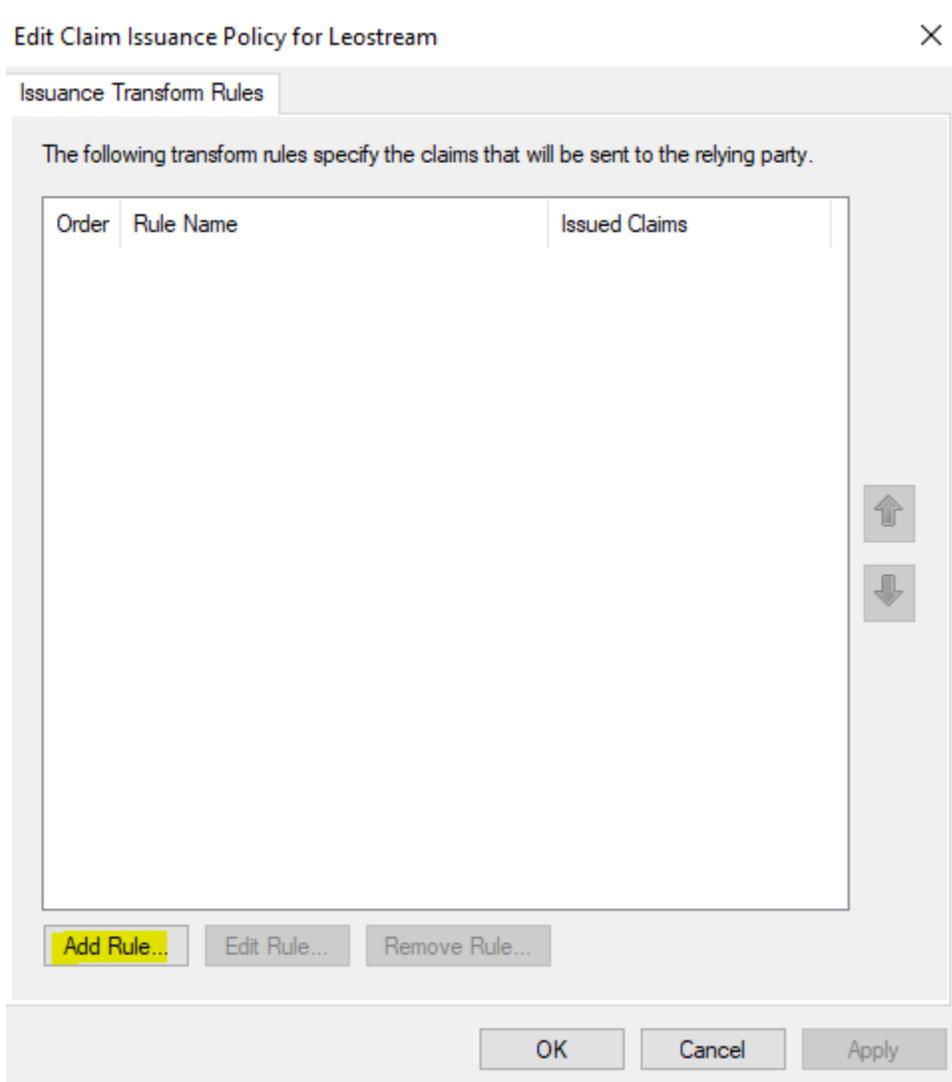
6. Select an appropriate **Display Name**, for example Leostream, as shown in the following figure.



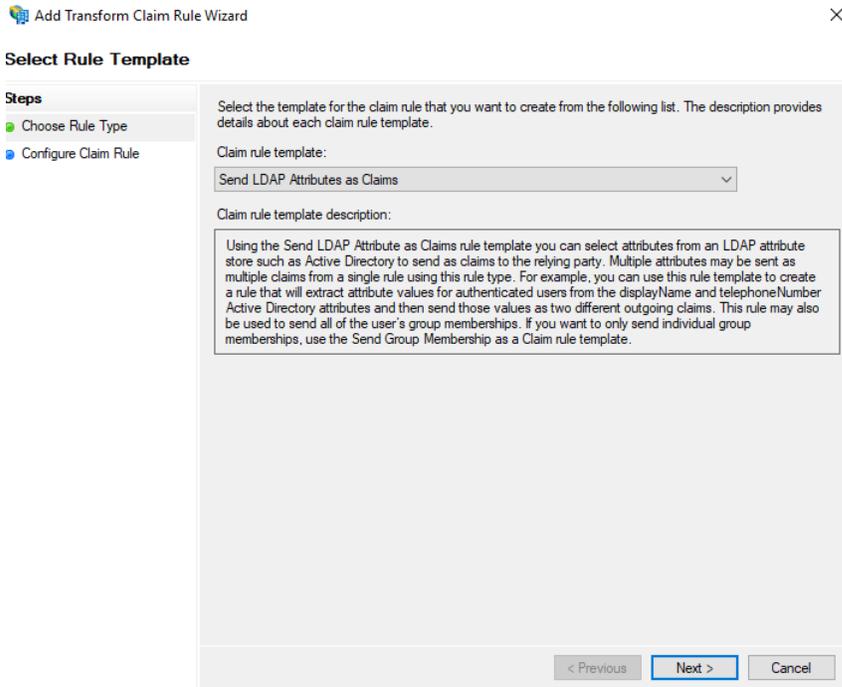
7. Click **Next**.
8. Select **Permit everyone** on the **Choose Access Control Policy** page



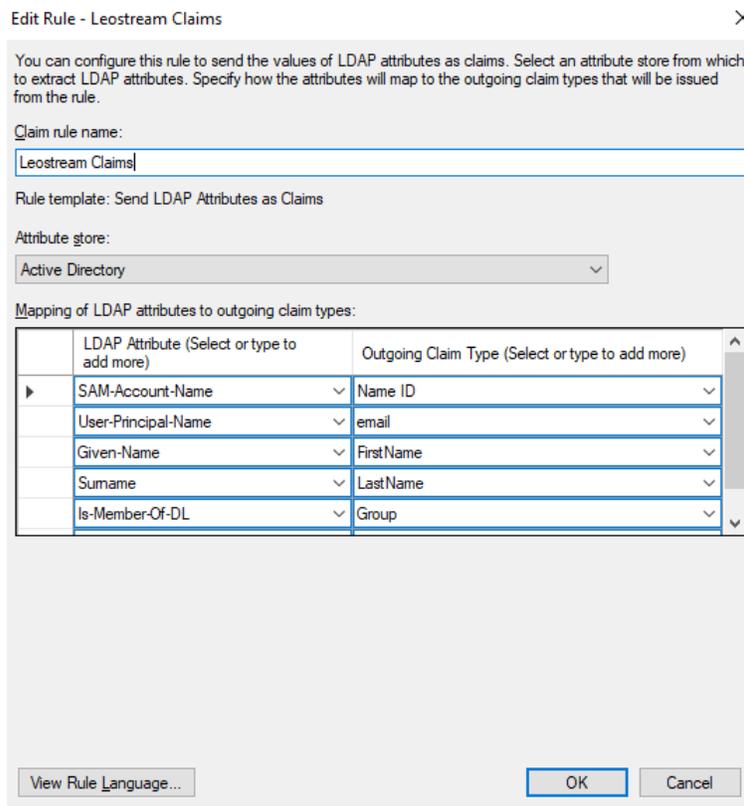
9. Click **Next**.
10. Click **Next** on the following page, then hit **Finish**.
11. Click **Close**. You should see a new dialog box appear to **Edit Claim Issuance Policy for Leostream**.
12. Click **Add Rule**, highlighted in the following figure.



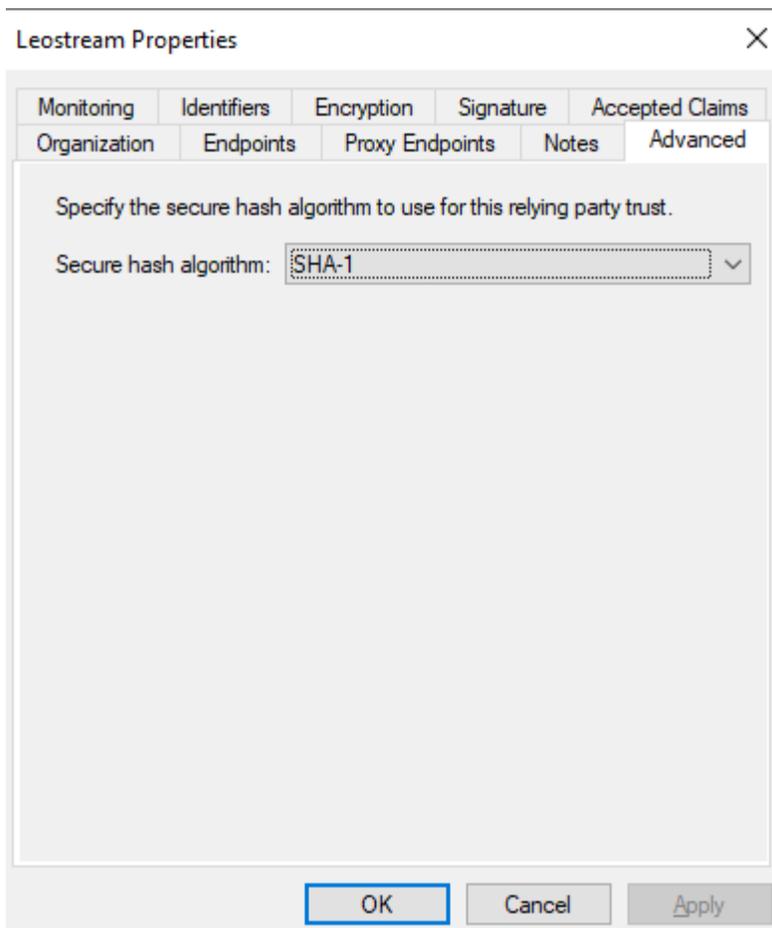
13. Select **Send LDAP Attributes as Claims** from the **Claim rule template** dropdown menu, shown in the following figure.



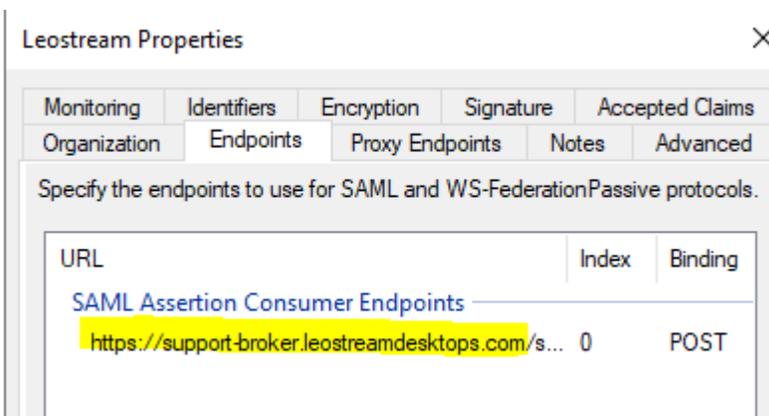
14. When configuring LDAP attributes for the outgoing claim on the next page, Leostream requires only the **Name ID** Outgoing Claim Type. However, the configuration in the following figure is the preferred minimum configuration to properly map the user's login name, email, first name, last name, and groups.

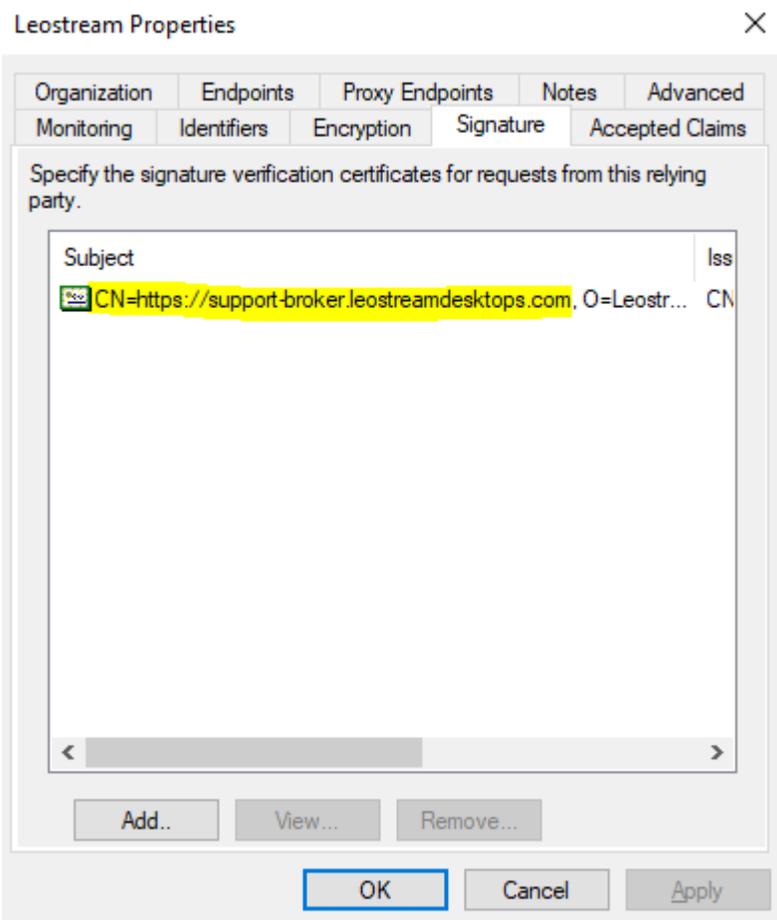


- Under the **Advanced** section of your Rely Party Trust properties, select **SHA-1** for the **Secure hash algorithm**, as shown in the following figure.



Ensure that the CN in the Signature matches the FQDN of the SAML Endpoint by comparing the value on the **Endpoints** tab, shown in the following figure, to the value on the **Signature** tab, shown in the subsequent figure.





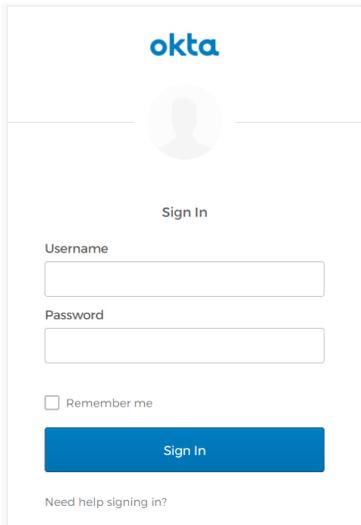
Example: SAML-logins with PCoIP Connections

The PCoIP Software Client version 21.01 introduces the feature to launch the client from a webpage using a URI. Leostream leverages this feature to launch PCoIP connections to desktops running the PCoIP Cloud Access Software from a Leostream Web client login.

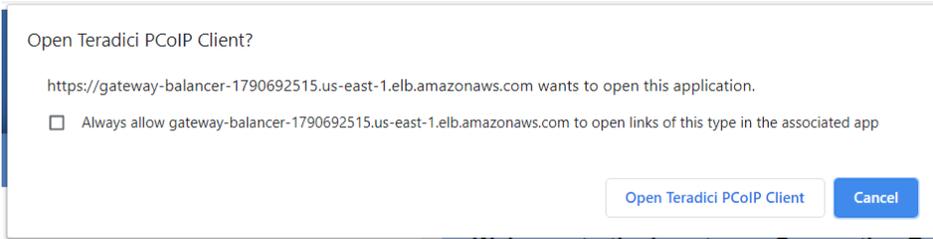
 This feature is not supported for PCoIP connections to Teradici Remote Workstation Cards unless the host desktop is running the PCoIP Cloud Access Software.

When using this feature, the user workflow is as follows.

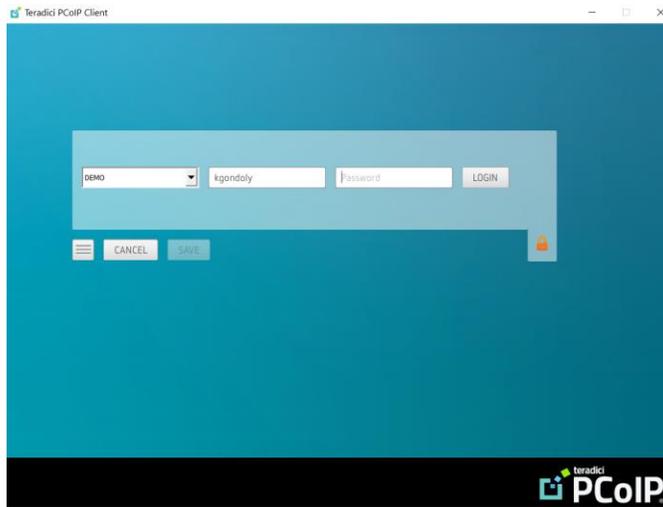
1. User authenticates with your SAML-based IdP, for example, Okta:



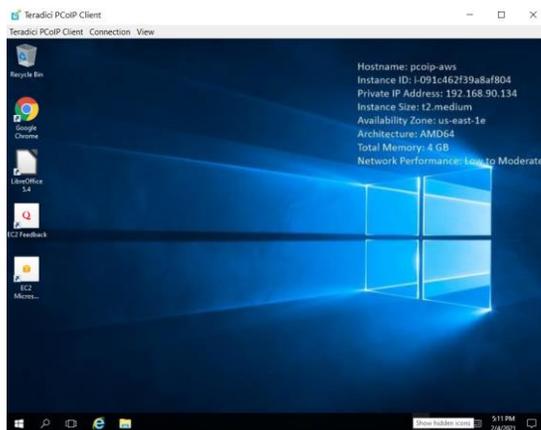
2. Successfully authenticated users are redirected to the Leostream Web client.
3. The Leostream Web client displays the list of offered desktops to the user.
4. The user clicks **Connect** on their desired desktops.
5. The Leostream Web client uses a URI to launch the PCoIP Soft client. Depending on the Web browser, the user may be prompted to accept the connection, for example:



- The PCoIP Cloud Access Software Agent on the remote desktop requires a username and password to authorize the connection. Therefore, the PCoIP Soft client launches and prompts for username/password credentials.



- For domain users, the Connection Broker validates the credentials against the Authentication Servers defined in the Connection Broker.
- If valid domain credentials or a local user were entered, those credentials are used to connect and log the user into the remote desktop. The credentials used to log into the remote desktop do not have to match those used to log into Leostream.



To enable this feature, configure your Protocol plan to launch the Teradici PCoIP Soft Client from a Web browser login, for example:

PCoIP Software Client Priority: ▾

Hostname or IP address of PCoIP Connection Manager

Send user domain as

Send user login name as

Desktop attribute to use for PCoIP connection

Use an IP address-based Dynamic Tag if the PCoIP Connection Manager or Client is unable to resolve the desktop's hostname

Enter the following information into this form.

- **Hostname or IP address of Teradici PCoIP Connection Manager** – The PCoIP connection must be established by your Teradici PCoIP Connection Manager. If the connection requires the Teradici Security Gateway, create a separate Protocol Plan for each Security Gateway in your environment. The Security Gateway entered in the Protocol Plan used in the user's Policy determines which Security Gateway manages the PCoIP traffic.
- **Send user domain as:** Enter the value to use as the default domain to display to the user in the PCoIP Soft client. The user will be able to select from this domain as well as any domain registered with your Connection Broker on the **> Setup > Authentication Servers** page.
- **Send user login name as:** Enter the value to use as the default username to display to the user in the PCoIP Soft client. The {USER} dynamic tag is replaced with the current user's login name returned in the SAML assertion.
- **Desktop attribute to use for PCoIP connection:** The PCoIP Connection Manager must be able to resolve the desktop's hostname. If that is not possible, modify this field to use an IP-address-based dynamic tag.

Use this protocol plan in the policy you will assign to users on the **Assignments** page for your SAML authentication server.

Example: Using Multiple SAML Servers

By default, the Connection Broker allows you to define a single SAML server for authenticating into your Leostream environment. If your organization uses multiple identity providers across different departments or business units, you can use the Leostream concept of *tenants* to define multiple SAML servers in your Connection Broker. This allows different groups of users to authenticate against different identity providers in order to gain access to your Leostream environment.



Your Leostream license key determines if you are able to add tenants to your Connection Broker. If your Connection Broker does not display the **> Setup > Tenants** menu, please contact sales@leostream.com to have the feature added to your Leostream Serial number. You must then generate and apply a new Leostream license key to your Connection Broker. Note that you may need to log out and back into the Connection Broker Administrator Web interface to see the **> Setup > Tenants** menu after applying your updated license key.

Step 1: Defining SAML Tenants

Each tenant in Leostream is defined by a unique fully qualified domain name (FQDN). Users for a particular tenant use their unique FQDN to access your Leostream environment. Each FQDN must resolve to the login portal for your Leostream environment, which may be the IP address or hostname of your Connection Broker or Leostream Gateway, or of the load balancer that manages traffic for your Leostream environment, depending on your architecture.

All tenants are managed by your top-level Connection Broker administrator. You can define sub-administrators for each tenant, who have permission to view the users and desktops currently in their tenant. Users and desktops become members of a particular tenant, as follows.

- Users become members of a particular tenant when they log into your Leostream environment from the FQDN defined for that tenant.
- Desktops become members of a tenant when 1) a user logs into a tenant and requests a connection to that desktop or 2) a Leostream pool provisions a desktop into a tenant. See **Extra: Sorting Desktops into Tenants** for more information.

Before defining tenants in your Connection Broker, ensure that you configure your DNS servers with your desired FQDNs, including one for each tenant and one for the top-level administrator, for example:

- corp.leostreamdesktops.com – The top-level administrator login
- sales.leostreamdesktops.com – Users in this tenant authenticate with Google Workspaces
- product.leostreamdesktops.com – Users in this tenant authenticate with Okta

To add tenants to your Connection Broker:

1. Log into your Leostream environment using a top-level administrator account, such as the default `admin` user.

2. Go to the > **Setup** > **Tenants** page.
3. Click **Add Tenant** at the top of the page.
4. In the **Add Tenant** form:
 - a. In the **Name** field, enter a descriptive name for your tenant. End users do not see this name.
 - b. In the **FQDN** field, enter the fully qualified domain name that end users will visit in order to log into your Leostream environment. For example:

5. Click **Save**.

After you add your first tenant, the **Tenants** drop-down menu appears at the top-right of your Connection Broker Administrator web interface, for example:

When the **Tenant** menu displays **Select...**, you are viewing the top-level Administrator interface. Use the **Tenant** drop-down menu to switch between tenants in order to define SAML servers, as described in the next section.

6. Repeat steps 3 through 5 for each of your tenants. Ensure that the **Tenant** drop-down menu continues to display **Select...** while you define all your tenants.

Step 2: Defining SAML Servers per Tenant

After you define your tenants, you can add SAML servers for each tenant in your Connection Broker. The value displayed in the **Tenant** drop-down menu at the time you add the SAML server determines which tenant that SAML server is associated with.

To add a SAML server for use with a particular tenant:

1. Log into your Leostream environment with a top-level administrator account, such as the default `admin` user. If you are already logged into the Administrator web interface ensure that the **Tenant** menu displays **Select...**
2. Go to the **> Setup > Authentication Servers** page.
3. From the **Tenant** menu at the top-right, select the tenant whose SAML server you need to add. The menu on the left of the Administrator Web interface updates to display only pages that are relevant to that tenant.
4. Click **Add Authentication Server**.
5. Select **SAML** from the **Type** drop-down menu and configure your SAML server as described in [Adding Your SAML IdP to Leostream](#).
6. Click **Save**.
7. From the **Tenant** menu at the top-right, select a different tenant whose SAML server you need to add. The menu on the left of the Administrator Web interface updates to display only pages that are relevant to that tenant and you no longer see the SAML server you defined for the previous tenant.
8. Repeat steps 4 through 7 for each tenant that requires a unique SAML server.
9. After you define SAML servers for all of your tenants, change the **Tenant** drop-down menu to display **Select...** The **> Setup > Authentication Servers** page displays all SAML servers for all tenant. If you need to define a SAML server to use for authenticating users into the top-level of your Leostream environment, add that SAML server while the **Tenant** drop-down menu displays **Select...**

After the SAML servers are registered in your Connection Broker, configure pools, plans, and policies using a top-level administrator account, then assign those policies to users via each SAML server's assignments table on the **> Configuration > Assignments** page.

Extra: Sorting Desktops into Tenants

Desktops that are not currently assigned to a particular tenant can be offered to any user, either at the top-level or in a tenant. After a desktop is a member of a particular tenant, the Connection Broker offers that desktop only to users in that tenant.

The Connection Broker automatically assigns a desktop to a tenant when a user who's logged into that tenant requests a connection to the desktop. You can manually assign desktops to tenants in three ways:

1. Use the **Import Desktop** option on the **> Resources > Desktop** page to register a new desktop with your Connection Broker. When registering the desktop, select the appropriate tenant from the **Assigned tenant** drop-down menu in the **Assignment** section of the **Import Desktop** form. After the desktop is registered, ensure that you install or restart the Leostream Agent on the desktop.
2. Assign existing desktops to a tenant by editing the desktop and selecting the appropriate tenant from the **Assigned tenant** drop-down menu in the **Assignment** section of the **Edit Desktop** form. You can select multiple desktops and use the **Bulk Edit** form, shown in the following figure, to simplify assigning a large number of desktops to a particular tenant.

The screenshot shows a window titled "Edit Desktops" with a help icon and a close icon. Below the title bar is the "Assignment" section. It contains a checkbox labeled "Forget previously-assigned user" which is unchecked. Below that are two dropdown menus. The first is labeled "Assign tenant:" and has "Sales" selected. The second is labeled "Log user into remote desktop as:" and has "No change" selected.

See the Connection Broker Administrators Guide for information on how to perform a bulk edit.

3. Provision new desktops into a particular tenant by selecting the tenant from the **Provision for tenant** drop-down menu in the **Provisioning** section of a pool. For example, the following figure provisions into the **Sales** tenant.

The screenshot shows a section titled "Provisioning". It has a checked checkbox labeled "Provisioning enabled". Below that is a dropdown menu labeled "Provision for tenant" with "Sales" selected.