LEOSTREAM™


# Integrating with SAML-Based Identity Providers

## Supporting Multi-factor Authentication for your Leostream Environment

**Version 9.0.38**
**November 2020**

## Contacting Leostream

Leostream Corporation
271 Waverley Oaks Rd.
Suite 204
Waltham, MA  02452
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



## 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

# 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, 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.

⚠ 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.

When enabled, all domain users should authenticate against the IdP in order to gain access to your Leostream environment.

# Preparing Your Identity Provider

When using a SAML IdP as the authentication portal for your Leostream environment, Leostream assigns policies to users based on the attributes contained in the hash 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 Metadata

How you obtain these values depends on which IdP you use.

# Preparing Leostream to Work with Your SAML IdP

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

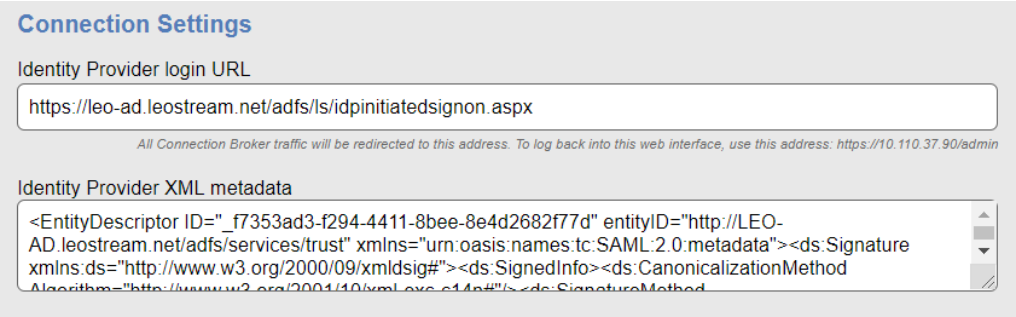
1. Go to the **> Setup > Authentication Servers** page.
2. Click the **Add Authentication Server** link.
3. Select **SAML** from the **Type** drop-down menu.

   ⚠ You can add a single SAML IdP to your Connection Broker. You will not see the **SAML** option in the **Type** drop-down menu if you already defined a SAML IdP. If you do not see the **SAML** option in

the **Type** drop-down menu and your **Authentication Servers** page does not already list a SAML IdP, contact **sales@leostream.com** to enable SAML IdP integration in your Leostream environment.

4. Enter a descriptive name in the **Authentication Server Name** field. Leave the **Domain** field empty.

5. In the **Connection Settings** section, shown in the following figure, enter the **Identity Provider login URL** and the **Identity Provider XML Metadata** associated with your identity provider.




6. Click **Save** to save the form.

# Registering Leostream with Your SAML IdP

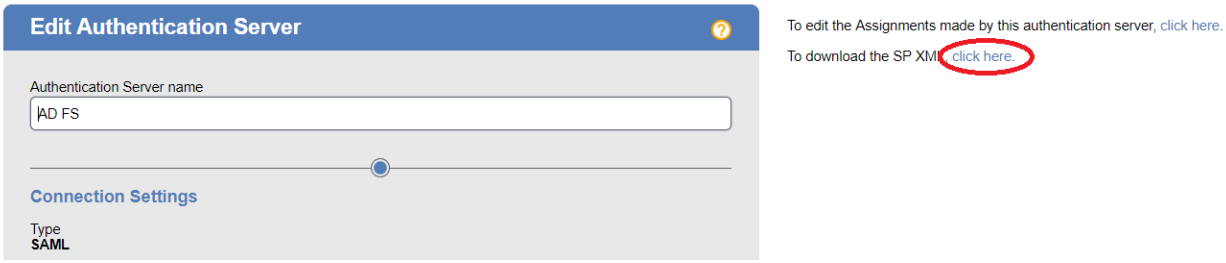
After saving your SAML authentication server, you must register your Leostream environment with your SAML IdP. Registering your Leostream environment allows your IdP to single sign-on your users into your Leostream environment via the Web client.

To continue, obtain the Service Provider (SP) XML for your Leostream environment, 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 SP XML downloads to a file named `leostream.xml`. Edit the file to optionally modify the following two parameters:

- `entityID = LeostreamBroker` – Edit this value if you want to change the entity name for the Leostream service provider you will register with your IdP.

- `Location = https://<broker_ip>/saml` – Where *<broker_ip>* is the IP address of the current Connection Broker. In clustered environments, edit this value so it is the VIP of your Leostream cluster.

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, all user 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.

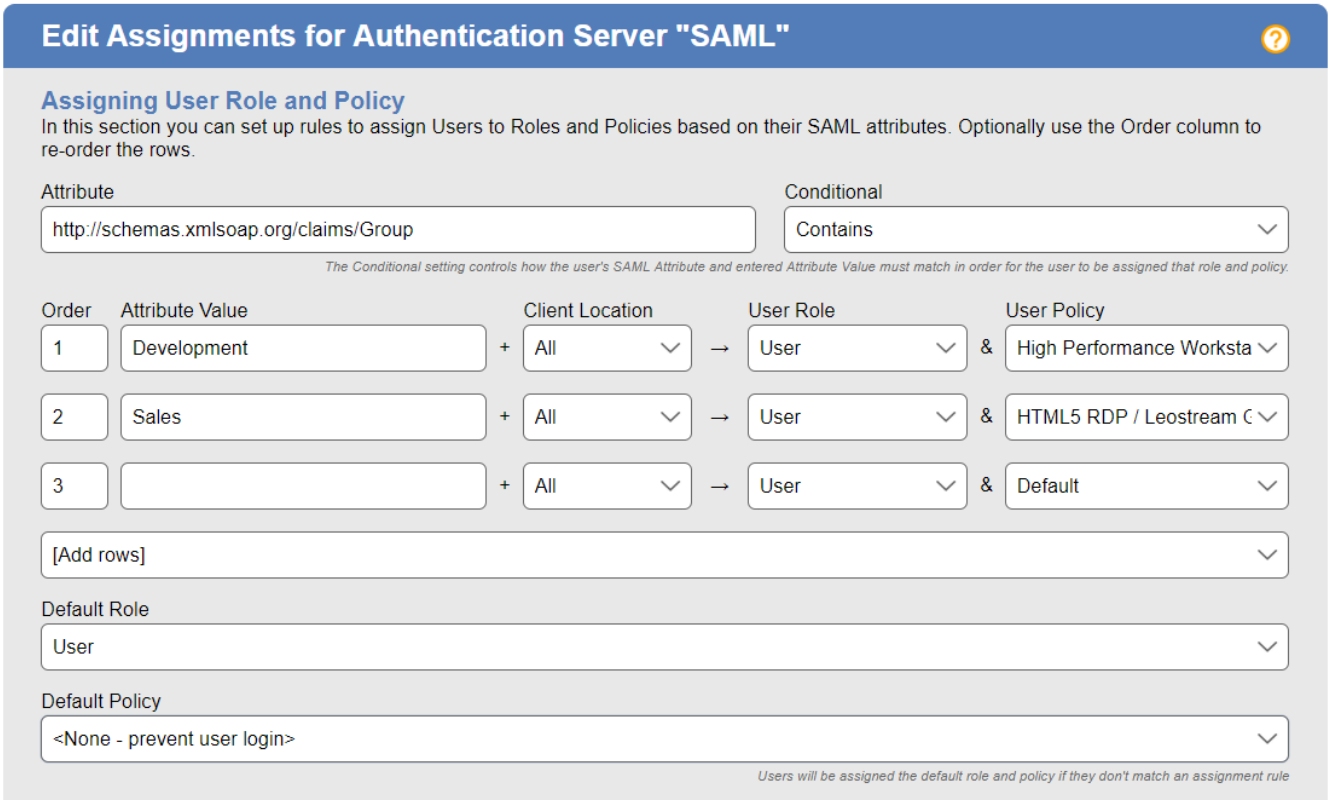
1. Go to the **> Configuration > Assignments** page in your Leostream Connection Broker.

2. Click **Edit** for your SAML IdP.

3. Enter the specific attribute Leostream to use for policy assignments into the **Attribute** edit field.

4. Select the appropriate **Conditional**, typically **Contains**.

5. In the **Attribute Value** field, enter the attribute to use for assigning policies. Your available attributes depend on the hash returned by your IdP. In the following figure, the **Group** attribute returns values of either **Development** or **Sales**.




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 as Administrators or Local Users

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

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

Where *`broker-address`* is the IP address or fully qualified host name of your Leostream environment.

To log into the administrator interface as the local administrator, as a domain user with an Administrator role, or to log in as a locally defined user, go to:

`https://broker-address/admin`

Where *`broker-address`* is the IP address or fully qualified host name of your Leostream environment.

# Controlling Access from other Client Types

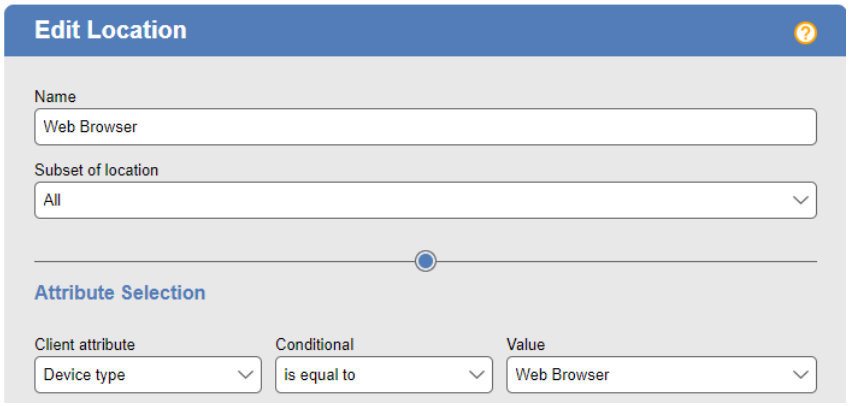
Users can log into Leostream from a variety of client types, including Web browsers, thin clients, zero clients, and Leostream Connect software clients. SAML-based authentication is available only for Web browser logins.

For other client types, you can use Leostream locations and assignment rules to determine if users are allowed to log in.

**Example 1: Blocking all direct Leostream logins for Domain Users**

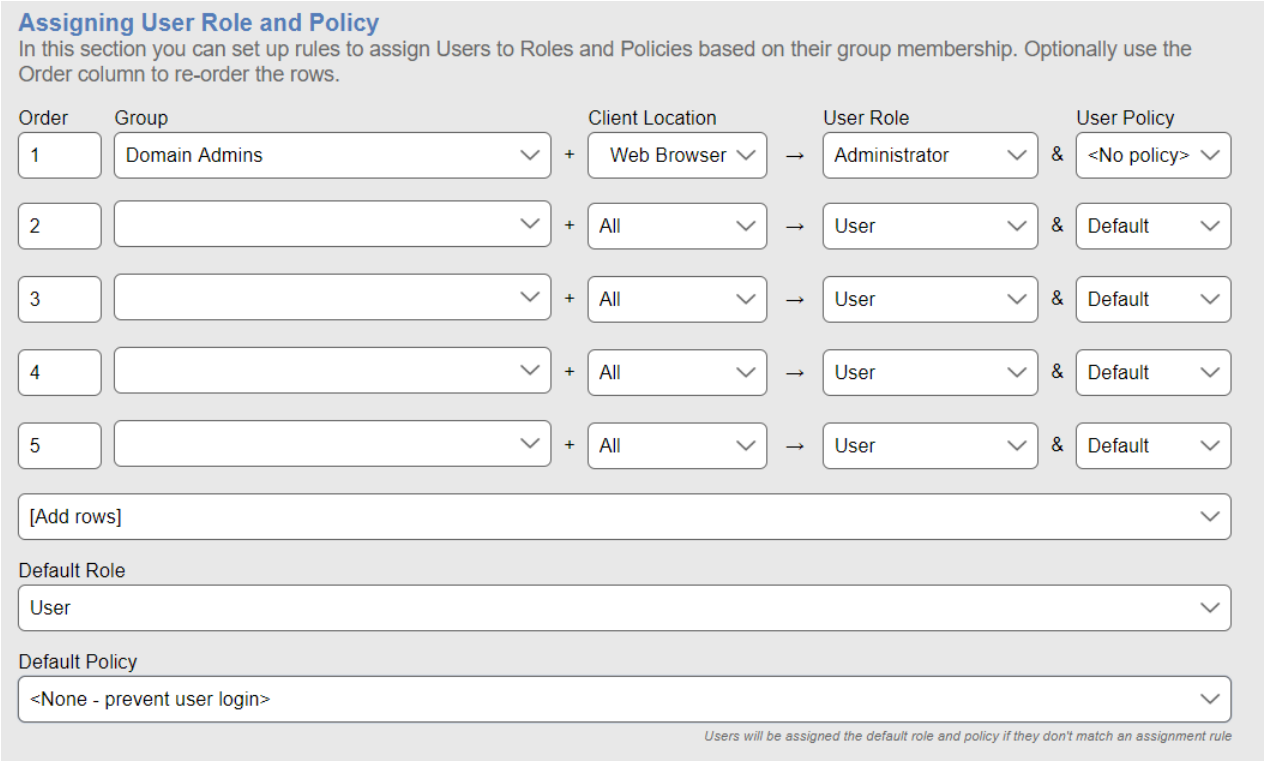
If you need to provide access to the Administrator Web interface for Domain users, but do not want Domain users to log in from any client type without authenticating with your SAML IdP, ensure that you configure the Assignments table for your Active Directory Authentication Server so it prevents domain user logins. To do this:

1) Create a location that includes all web browsers, for example:



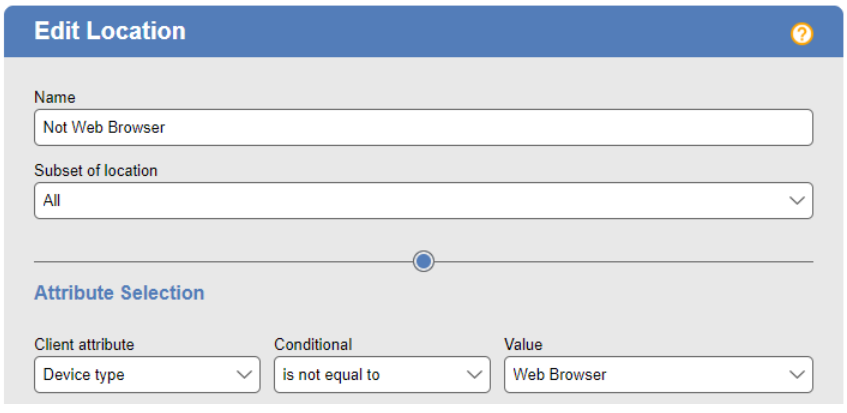

2) Configure the Assignments table to assign a Role that provides administrator access from this location, but no Policy.

3) Deny access othewise, by setting the **Default Policy** to **<None - prevent User Login>**, for example:

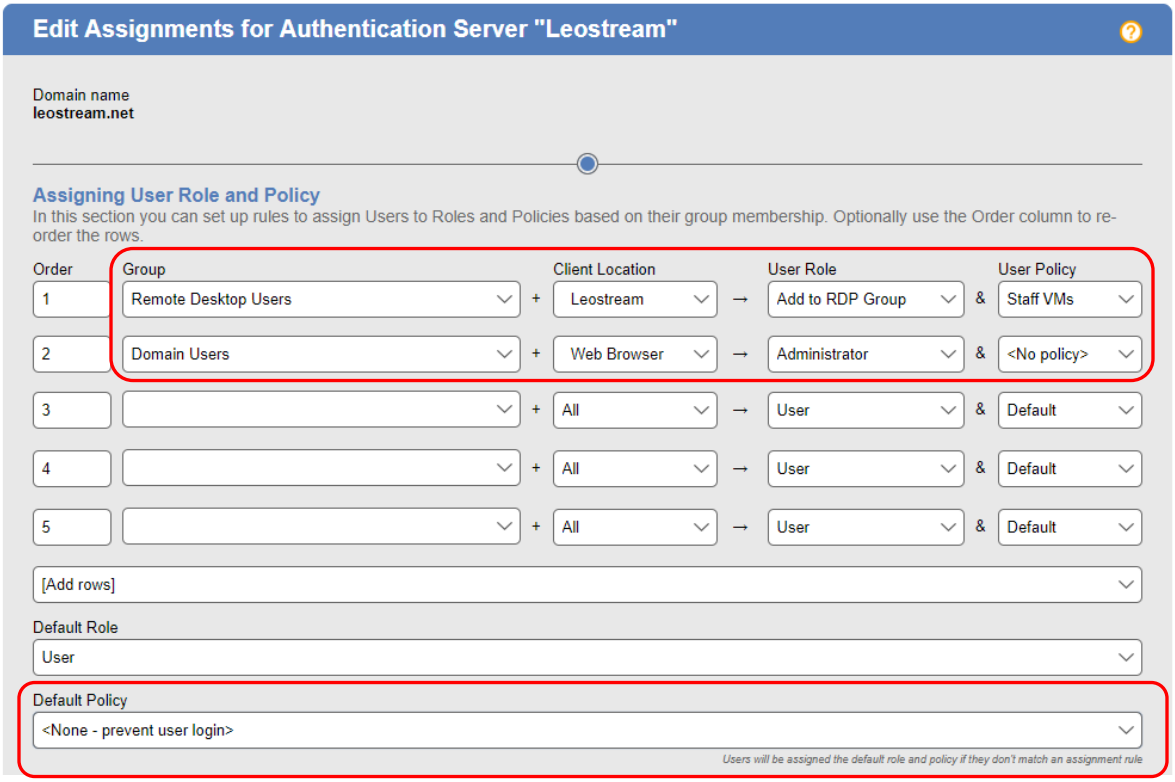



**Example 2: Allow direct Leostream logins for Domain Users from non-Web browser clients types**

To allow Domain users to log in from other client types, you can create a Leostream Location for all non-Web browser clients, for example:



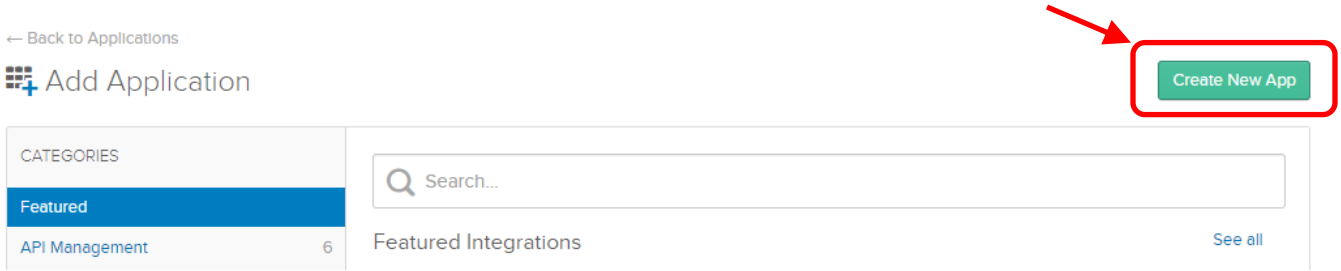

Use the Assignments table to assign a policy to users logging in from this location, allow Administrator access from the Web browser location, and block all other access, for example:




# 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 **Add Application** button.
4. In the **Add Application** page, click the **Create New App** button located at the top right, indicated in the following figure.



5. In the **Create a New Application Integration** form:

    a. Select **Web** from the **Platform** drop-down menu.
    b. Select **SAML 2.0** in the set of **Sign on method** radio buttons.
    c. Click **Create**.

6. 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**.

7. Pay attention to the following fields on the second page of the **Create SAML Integration** form. Any field that is not listed may be left at its default value.

    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 URL (SP Entity ID)** field, enter `LeostreamBroker`.

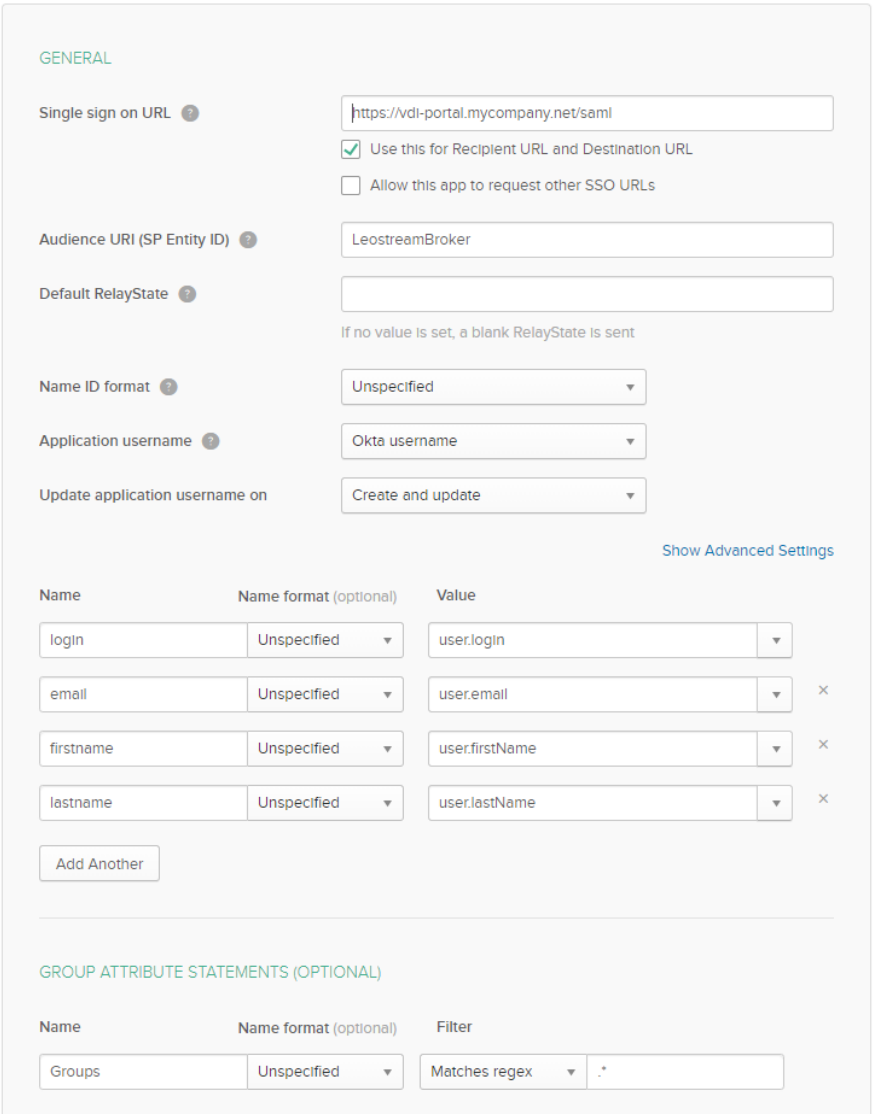
8. Enter the user attributes that Okta sends to Leostream in the SAML assertion that follows a successful Okta login. The user and group attributes represent the values you can use to assign policies in Leostream. The following table describes an example that sends the user's login name, email address, 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 |

9. 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:

a. **Name**: Groups
b. **Name forma**t: Unspecified
c. **Filter**: Matches regex
d. **Filter text**: .*

The following figure shows an example setup.

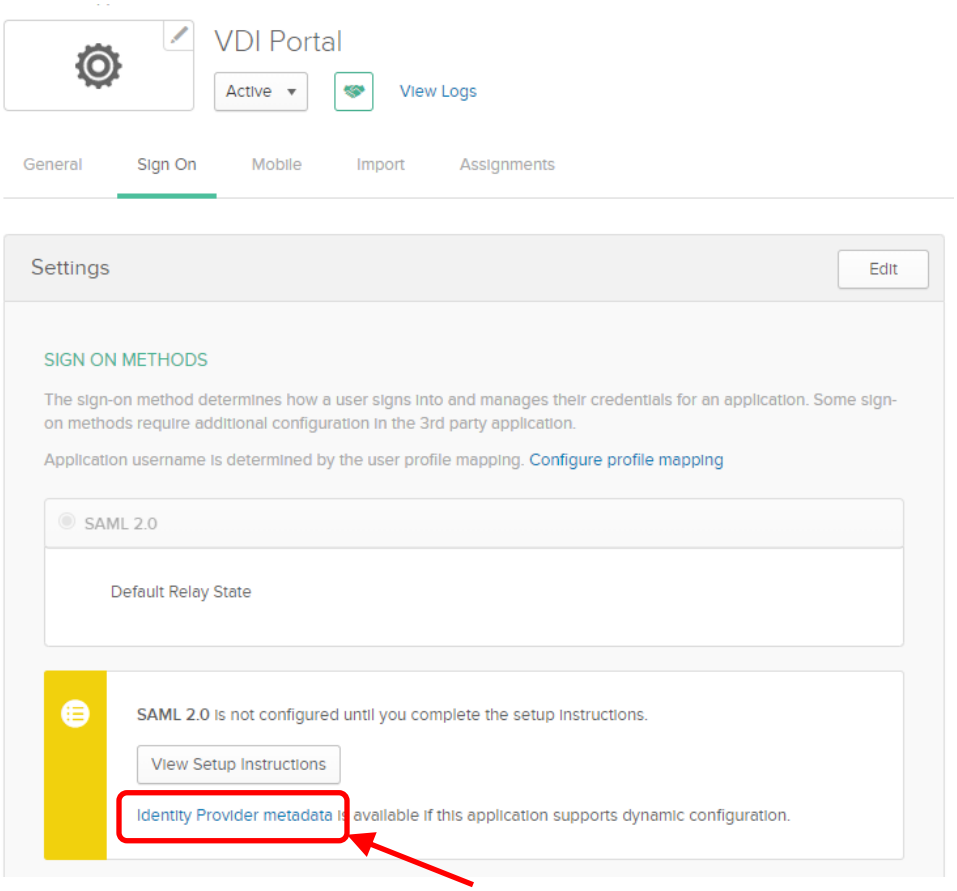



10. Click **Next** in this page of the **Create SAML Integration** form

11. 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, click the **Identity Provider metadata** link to obtain the information you need to add the SAML Authentication Server to your Leostream Connection Broker. You can find the **Identity Provider metadata** link on the **Sign On** tab of your SAML 2.0 application, indicated in the following figure.




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 near the end of the XML metadata. The URL takes a form similar to the following:

https://mycompany.okta.com/app/mycompany _vdiportal_1/exk6h9lfjuhw2wzeP357/sso/saml

Your URL will differ based on the name of your company's Okta portal, the name of your SAML 2.0 application, and the unique ID associated with that application.

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.html` 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