LEOSTREAM™

Integrating with SAML-Based Identity Providers

Supporting Multi-factor Authentication for your Leostream Environment

Version 9.0
August 2019

Contacting Leostream

Leostream Corporation
271 Waverley Oaks Rd.
Suite 206
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

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.

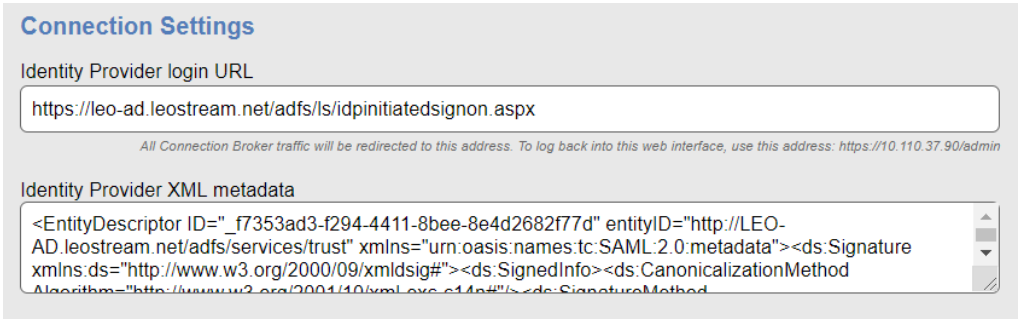
1. Go to the **> Setup > Authentication Servers** page.
2. Click the **Add Authentication Server** link.
3. Select **SAML** from the **Type** drop-down menu.

   ⚠ 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

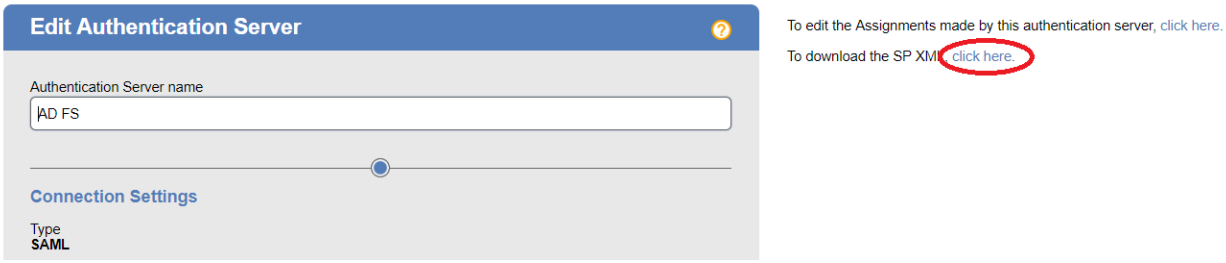
After saving your SAML authentication server, you must register your Leostream environment with your SAML IdP. Registering your Leostream environment allows your IdP to single sign-on your users into your Leostream environment via the Web client.

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.

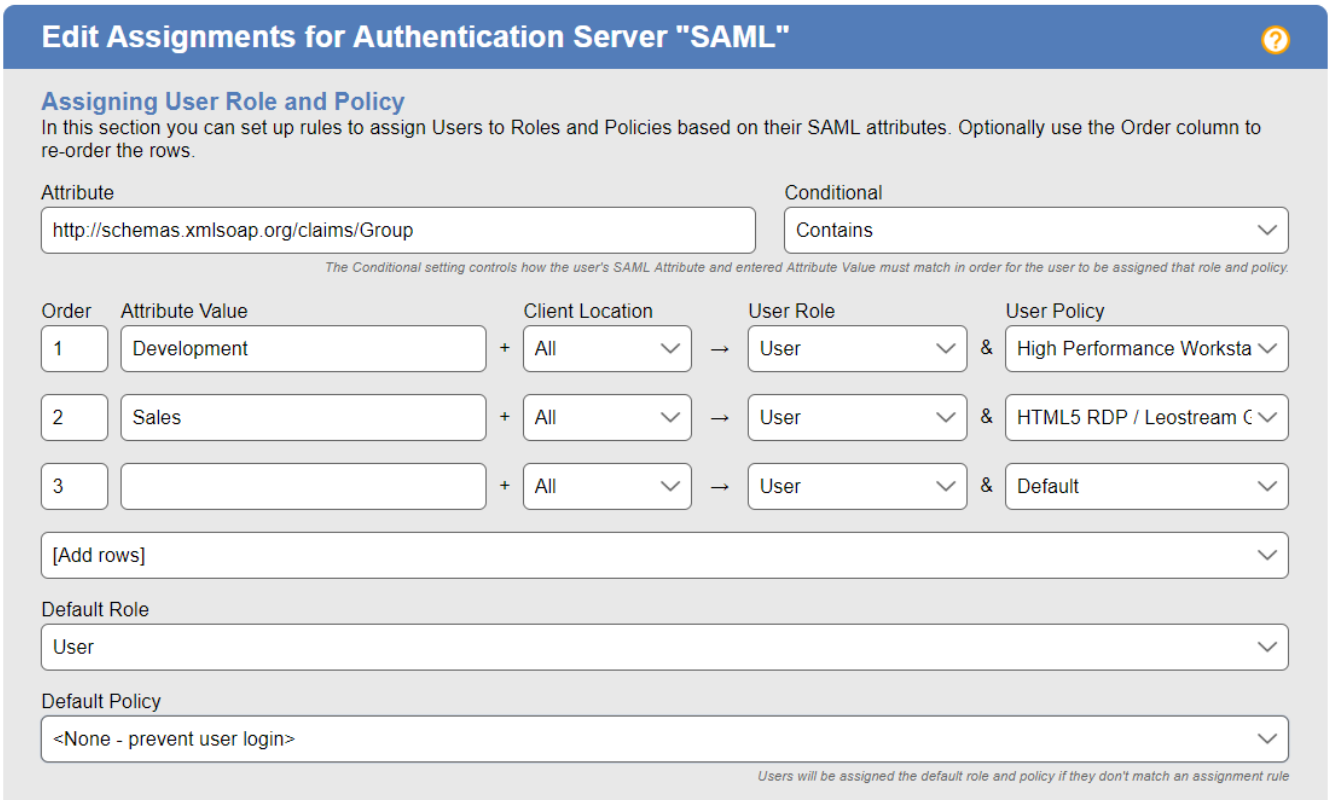
1. Go to the **> Configuration > Assignments** page in your Leostream Connection Broker.

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

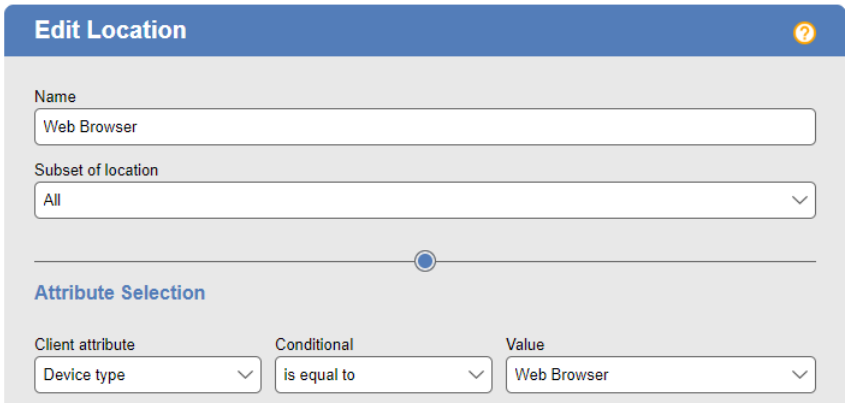
Users can log into Leostream from a variety of client types, including Web browsers, thin clients, zero clients, and Leostream Connect software clients. SAML-based authentication is available only for Web browser logins.

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

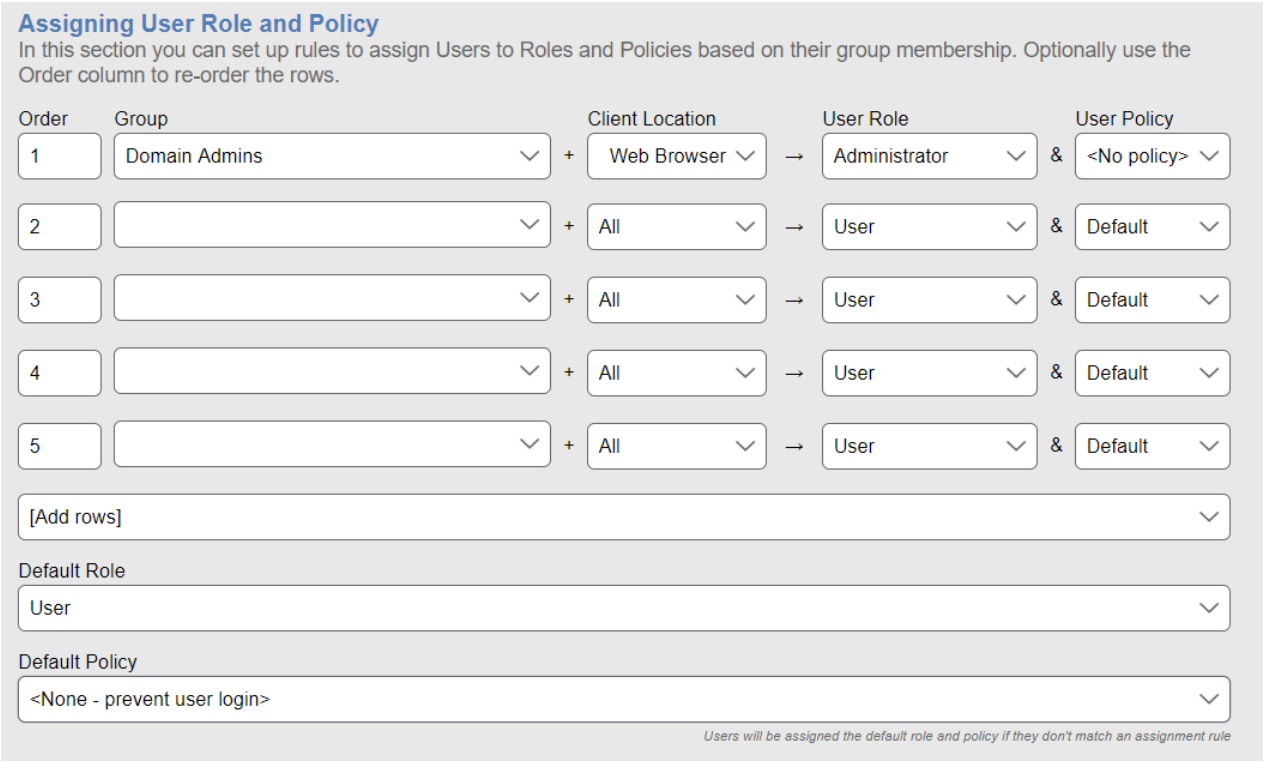
If you need to provide access to the Administrator Web interface for Domain users, but do not want Domain users to log in from any client type without authenticating with your SAML IdP, ensure that you configure the Assignments table for your Active Directory Authentication Server so it prevents domain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

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



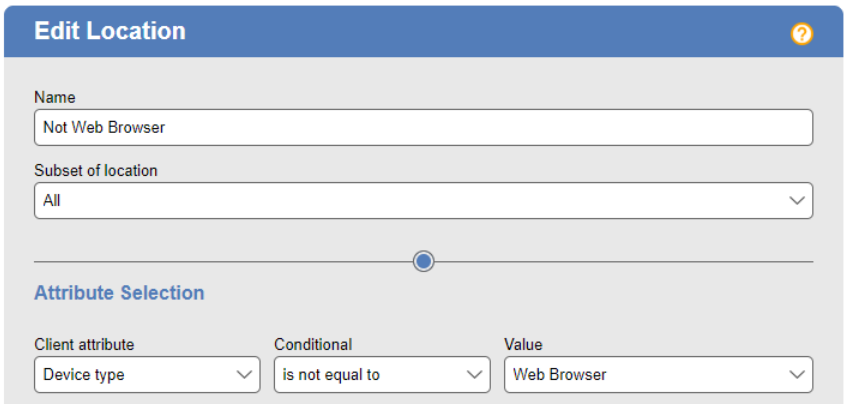
2) Configure the Assignments table to assign a Role that provides administrator access from this location, but no Policy.

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

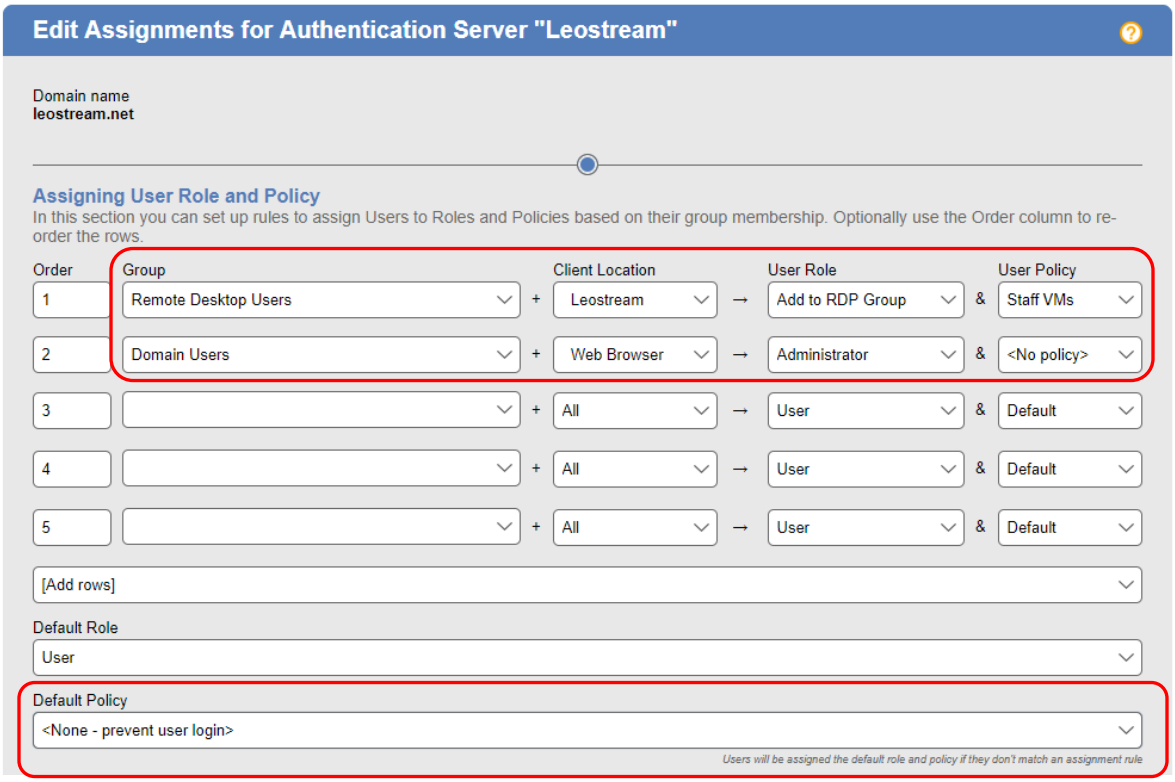


Example 2: Allow direct Leostream logins for Domain Users from non-Web browser clients types

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:


Edit Assignments for Authentication Server "Leostream"
Domain name
leostream.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
User Role
User Policy
1
Remote Desktop Users
+
Leostream
→
Add to RDP Group
&
Staff VMs
2
Domain Users
+
Web Browser
→
Administrator
&
<No policy>
3
+
All
→
User
&
Default
4
+
All
→
User
&
Default
5
+
All
→
User
&
Default
[Add rows]
Default Role
User
Default Policy
<None - prevent user login>
Users will be assigned the default role and policy if they don't match an assignment rule