



# leostream<sup>®</sup>

Remote Desktop Access Platform

## **Integrating the Leostream<sup>®</sup> Platform with Microsoft Entra ID as a SAML Provider**

**Adding Azure Multi-Factor Authentication to your Leostream Environment**

## 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](mailto:features@leostream.com).

To request product information or inquire about our future directions, email [sales@leostream.com](mailto:sales@leostream.com).

## Copyright

© Copyright 2002-2024 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 or registered 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

<b>Contents.....</b>	<b>3</b>
<b>Overview .....</b>	<b>4</b>
<b>Preparing Microsoft Entra ID .....</b>	<b>4</b>
<b>Configuring the Connection Broker to Work with Entra ID .....</b>	<b>8</b>
<b>Final Configuration steps in Microsoft Entra ID .....</b>	<b>9</b>
<b>Assigning Policies for Microsoft Entra ID Logins.....</b>	<b>11</b>
<b>Enabling Azure MFA for Entra ID SAML Logins .....</b>	<b>13</b>

## Overview

The Leostream® Platform allows you to leverage Microsoft Entra ID as a SAML-based Identity Provider (IdP) to provide single sign-on to the Leostream web client with multi-factor authentication. In order to do so, you must create an Enterprise Application in your Azure Portal.

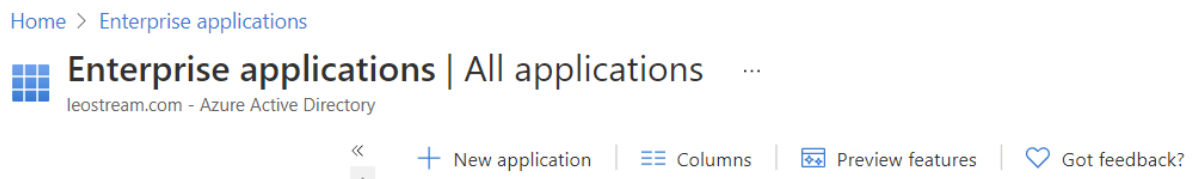
After enabling Leostream to work with your Entra ID, end users authenticate against Azure using the SAML protocol to provide single sign-on for the user into your Leostream environment. This also allows you to utilize Azure MFA by leveraging Azure Conditional Access policies.

 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.

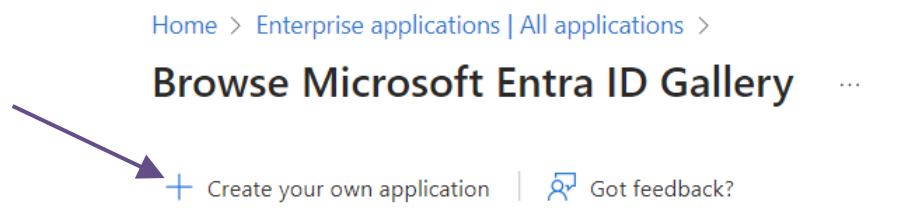
## Preparing Microsoft Entra ID

When using Entra ID as the SAML authentication portal for your Leostream environment, the Connection Broker assigns policies to users based on the attributes contained in the hash returned by Entra ID. Before you can describe the attributes returned to your Connection Broker for policy assignment, you must create an Enterprise Application that acts as the integration point between your Leostream platform and Entra ID, as follows.

1. In your Azure portal, go to > **All services > Enterprise applications**.



2. In the **All applications** list, click **New Application**.
3. In the **Browse Microsoft Entra ID Gallery** window, click **Create your own application**, indicated in the following figure.



4. In the **Create your own application** pane:

- a. Enter a name for your application.
- b. Select **Integrate any other application you don't find in the gallery**, for example:

### Create your own application

✕

Got feedback?

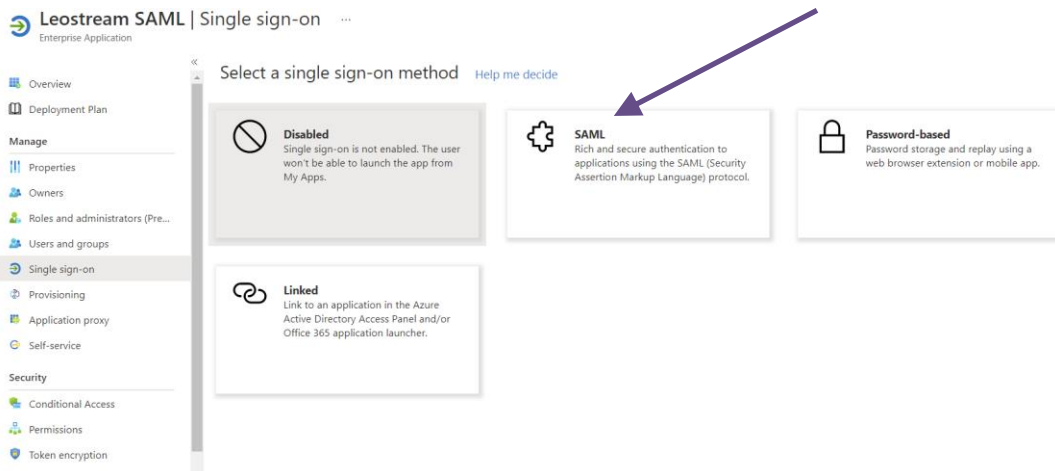
If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application  
☐ Register an application to integrate with Microsoft Entra ID (App you're developing)  
☒ Integrate any other application you don't find in the gallery (Non-gallery)

- c. Click **Create**. After the application is created, your Azure portal displays the **Overview** pane for your new application.
5. In the **Getting Started** section of the **Overview** pane, click the **Get started** link in option **2. Set up single sign on**.
  6. In the **Select a single sign-on method** pane, shown in the following figure, click the **SAML** tile.



7. In the **Set up Single Sign-On with SAML** pane, click the **Edit** link associated with the **Basic SAML Configuration**, indicated in the following figure.

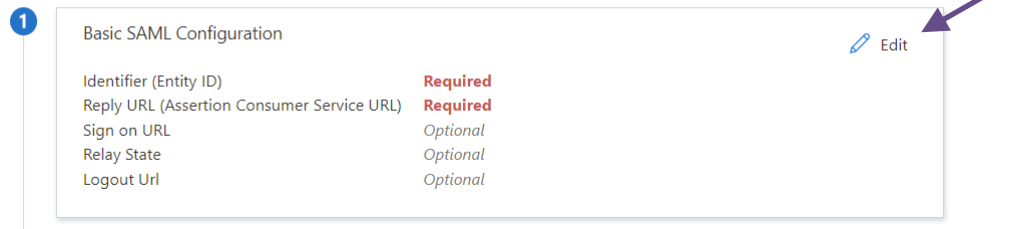
### Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Karen SAML.

1

Basic SAML Configuration Edit

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>





8. In the **Basic SAML Configuration** pane:

- In the **Identifier (Entity ID)** section, click the **Add identifier** link and then enter the Entity ID to use for your Leostream Connection Broker. The Entity ID must be unique across your organization. Note this value down for later as you will use it when setting up your Leostream Connection Broker to communicate with Entra ID.
- In the **Reply URL (Assertion Consumer Service URL)** section, click the **Add reply** URL link and enter your Leostream address with `/saml` added at the end of the URL. This is the URL Azure will use for the SAML assertions that log users in after they authentication with Microsoft Entra ID.
- Enter the same URL for the **Sign on URL**.

The following figure shows an example Entity ID and Reply and Sign on URLs. In this example, the Leostream Sign on URL is the Leostream Gateway address. To determine how to set the Sign on URL for your environment, consult the “Determining your Leostream Single Sign-On URL” in the Leostream Guide for [Using SAML-Based Identity Providers with the Leostream Platform](#).

## Basic SAML Configuration


 Save |  Got feedback?

---

Identifier (Entity ID) \* ⓘ

*The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.*


Default

✓ ☒ ⓘ 

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) \* ⓘ

*The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.*

	Index	Default
<input type="text" value="https://leostream_gateway.leostream.net/saml"/> ✓	<input type="text"/>	<input checked="" type="checkbox"/> ⓘ 

[Add reply URL](#)

Sign on URL (Optional)

*Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.*

✓

- d. Leave the **Relay State** and **Logout Url** blank and click the **Save** icon at the top-left of the pane to save the Basic SAML Configuration.
9. In section 3 of the **Set up Single Sign-On with SAML** pane, click the **Download** link associated with the **Federation Metadata XML**, indicated in the following figure.
10. Finally, in sections 4, copy the **Login URL**, also indicated in the following figure.

## Configuring the Connection Broker to Work with Entra ID

After building your Enterprise Application in Azure, register it with your Leostream platform by creating a SAML 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.



You can add a single SAML IdP to your Connection Broker. Therefore, 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](mailto:sales@leostream.com) to enable SAML IdP integration 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 you specified when creating the Enterprise Application in Azure.
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, for example:

- a 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 exactly LastName and FirstName must be returned as attributes in the SAML assertion
- b For **Email address**, enter {SAML:http://schemas.xmlsoap.org/claims/email} if the email attribute is returned in the SAML assertion as a URI reference.

7. In the **Connection Settings** section, shown in the following figure:

- a Enter the **Login URL** you copied from your Enterprise Application into the **Identity Provider login URL** field.
- b Enter the **Federation Metadata XML** you downloaded from your Enterprise Application into the **Identity Provider XML Metadata** field.



The screenshot shows the 'Connection Settings' section of a form. It contains two main input fields. The first is labeled 'Identity Provider login URL' and has a text box below it. Below the text box is a note: 'All Connection Broker login traffic will be redirected to this address'. Below the note is a checkbox labeled 'Enable user logins without SAML at "https://10.110.37.22/login"' with a sub-note: 'Connection Broker administrators can always log in at "https://10.110.37.22/admin"'. The second input field is labeled 'Identity Provider XML metadata' and has a large text box below it.

8. By default, after you created a SAML-based authentication server, the Connection Broker redirects all users to the Identity Providers login URL when the user visits the Connection Broker login page. To allow users to bypass the SAM-based authentication server, select the **Enable user logins without SAML** check box. See “Enabling Username and Password Logins” in the Leostream Guide for [Using SAML-Based Identity Providers with the Leostream Platform](#) for more information.

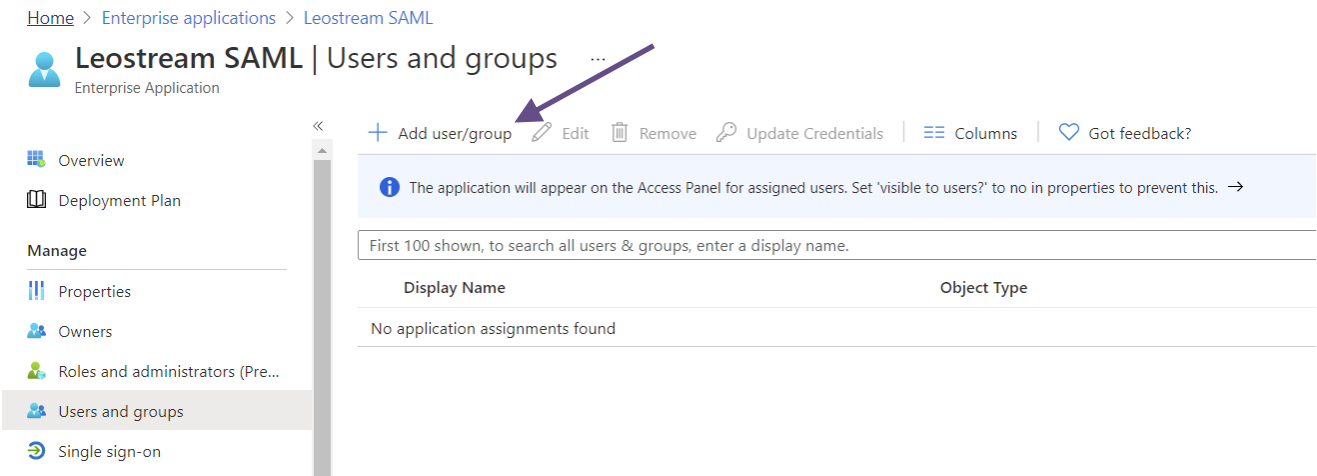
9. Click **Save** to save the form.

## Final Configuration steps in Microsoft Entra ID

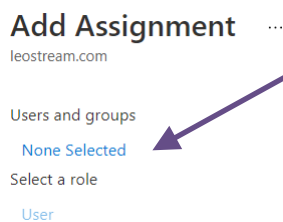
After saving your SAML authentication server in your Connection Broker, return to your Azure portal to indicate which users may access the Enterprise Application created for your Leostream environment.

1. In your Azure portal, go to > **All services** > **Enterprise applications** pane.
2. Select your Leostream Enterprise Application from the **All applications** list.

3. From the menu on the left, select **Users and groups**.
4. In the **Users and groups** pane, shown in the following figure, click the **Add user/group** link to indicate which Entra ID users and groups are allowed to log into your Leostream environment.



5. In the **Add Assignment** pane, click the **None Selected** link below the **Users and groups** header to open the pane where you can add users and groups to this application.

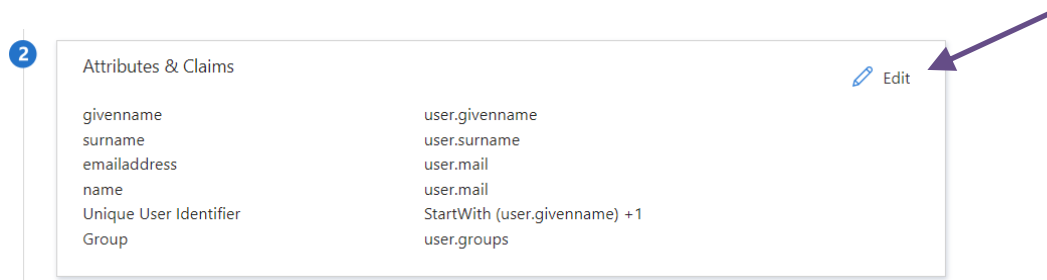


6. In the **Users and groups** pane, click the users and groups to assign to your Leostream environment and click **Select**.
7. After you have selected all your users and groups, click the **Assign** button at the bottom of the **Add Assignments** pane to complete the assignments.


By default, Entra ID does not share group data via the SAML assertion sent to your Connection Broker. To assign Leostream policies based on group membership, you must alter the **User Attributes & Claims** section of your Leostream Enterprise Application.

1. In your Azure portal, go to > **All services > Enterprise applications** pane.
2. Select your Leostream Enterprise Application from the **All applications** list.

3. In the **Getting Started** section of the **Overview** pane, click the **Get started** link in option **2. Set up single sign on**.
4. Click the **Edit** link in section **2. Attributes & Claims**, shown in the following figure, to add group claims to the SAML assertion.



5. In the **User Attributes & Claims** pane, click **Add a group claim**.
6. In the **Group Claims** pane, use one of the available options to select which groups to return in the SAML assertion. For example, you can select **Groups assigned to the application** to send all the groups you assigned to your Enterprise application in the previous procedure.

 If you have more than 150 groups, ensure that you send only the groups that you plan to use to assign Policies in your Leostream Platform. Microsoft Entra ID limits the number of groups that it will return in a SAML assertion to 150. Therefore, you cannot assign Policies in Leostream to more than 150 groups of Entra ID users.

7. Select **Group ID** from the **Source attribute** drop-down menu, as shown in the following figure.
8. Click **Save**.

After adding group attributes to the SAML assertion, your users can login to Leostream by going to the web address of your Leostream environment. The next section describes how to assign a Leostream policy to your users, to control what resources they have access to in your environment.

## Assigning Policies for Microsoft Entra ID Logins

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

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

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

- Click **Edit** on your Entra ID Authentication Server.
- Enter the specific attribute the Connection Broker uses for policy assignments in the **Attribute** edit field. For Entra ID, the attribute is the full URL claim name shown in the **User Attributes & Claims** pane. For example, to use the Entra ID groups added to the SAML assertion in the previous section, the attribute takes the form:

```
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
```

- Select the appropriate **Conditional**, typically **Contains**.
- In the **Attribute Value** field, map values of the attribute to the appropriate Leostream roles and policies. The Entra ID SAML assertion returns group information as the Object ID of the Entra ID Group. To locate the Object IDs for your Azure groups, go to the **> All services > Groups** page in your Entra ID portal.

### Edit Assignments for Authentication Server "Microsoft Entra ID"

**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

http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Exactly matches

*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	5170927d-e811-4bf9-8d98-222f8fb532c	+ All	→ User	& Default
2		+ All	→ User	& Default
3		+ All	→ User	& Default

[Add rows]

Default Role

User

Default Policy

Default

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

- 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 Entra ID, 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.

## Enabling Azure MFA for Entra ID SAML Logins

To use Azure MFA for your Leostream Enterprise Application, use the **Microsoft Entra Conditional Access** service in your Azure Portal.

1. In your Azure portal, go to **> All services > Microsoft Entra Conditional Access** pane.
2. In the **Conditional Access > Policies** pane, click **New policy**.
3. In the **Assignments** section of the **New** Conditional access policy pane, click the link below the **Users** header to select the users/groups that are required to use MFA.
4. Below the **Target resources** header, click the link to associate your Leostream Enterprise Application with this new conditional access policy.
  - a Select **Cloud apps** from the **Select what this policy applies to** options.
  - b Select **Select apps** from the **Include** options.
  - c Select your Leostream Enterprise Application from the list of available applications and click **Select**.
5. Click the link below the **Conditions** header to define the conditions and access controls according to your organizations MFA policy.
6. Click **Create** to enable the Conditional Access Policy.

After the policy is enabled, users are required to authenticate with Entra ID in order to login to your Leostream application. Leostream recommends testing with a small group of users, to confirm the correct behavior of your conditional access policy.