LEOSTREAM™

Integrating Leostream with Azure Active Directory as a SAML Provider

Adding Azure Multi-Factor Authentication to your Leostream Environment

Version 9.1
October 2021

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

Patents

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

Contents

Overview

Leostream 9 allows you to leverage Azure Active Directory 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.

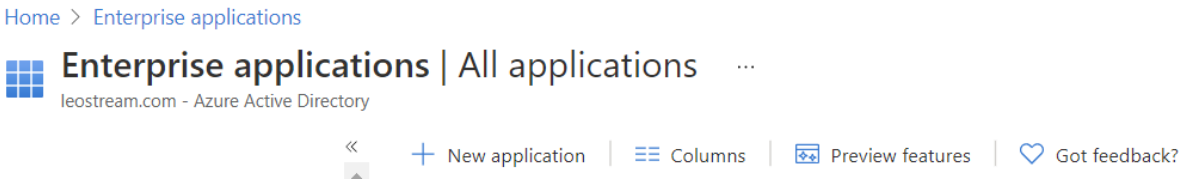
After enabling Leostream to work with your Azure AD, end users authenticate against Azure using the SAML protocol to provide single sign-on for the user into your Leostream environment. This also allows you to utilize Azure MFA by leveraging Azure Conditional Access policies.

⚠ 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 Azure AD to Work with Leostream

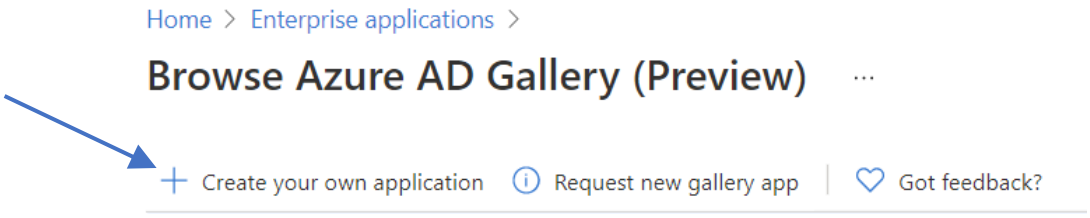
When using Azure AD as the SAML authentication portal for your Leostream environment, Leostream assigns policies to users based on the attributes contained in the hash returned to Leostream by your Azure AD. Before you can describe the attributes returned to Leostream for policy assignment, you must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

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



2. In the **All** applications list, click **New Application**.

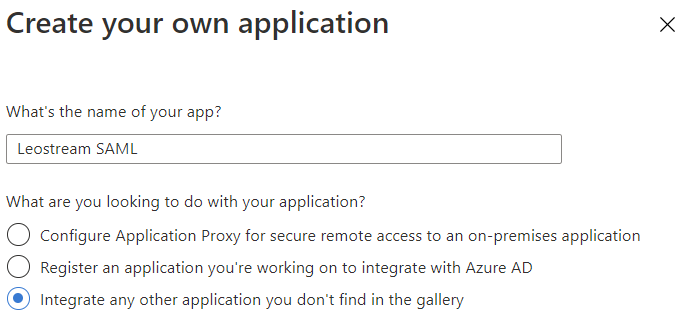
3. In the **Browse Azure AD Gallery** window, click **Create your own application**, indicated in the following figure.



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

    a. Enter a name for your application.

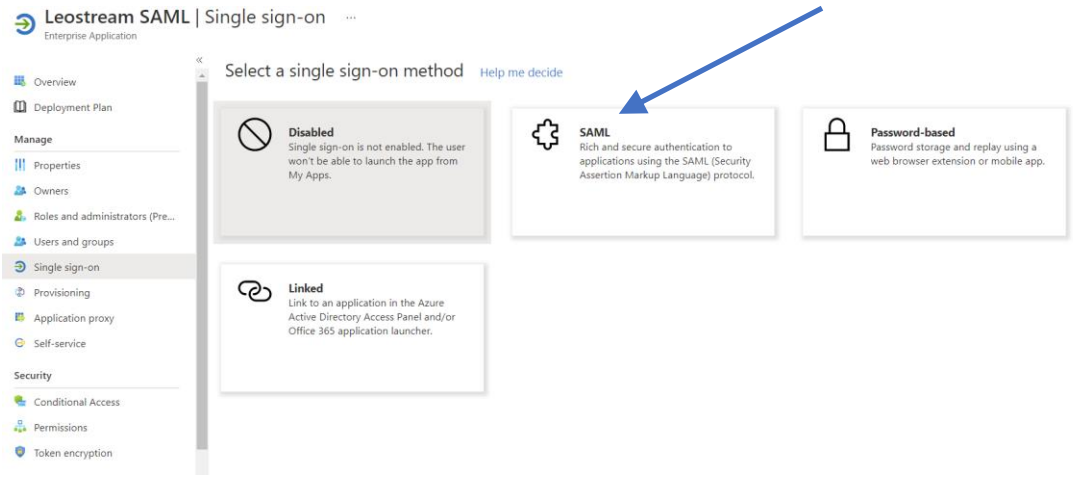
b. Select **Integrate any other application you don't find in the gallery**, for example:



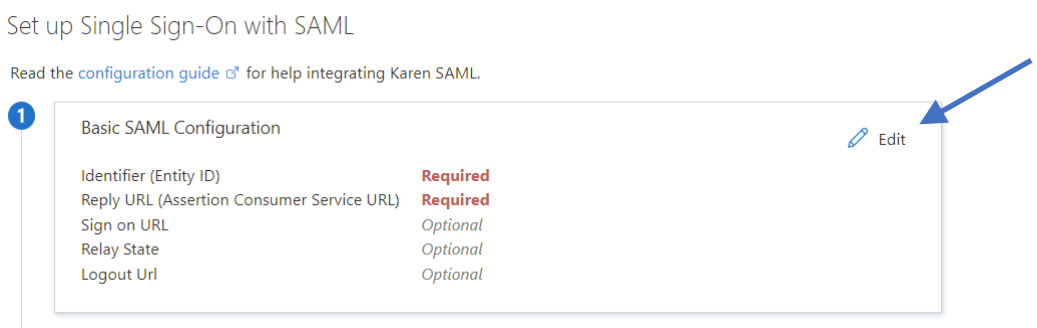
c. Click **Create**. After the application is created, your Azure portal displays the **Overview** pane for your new application.

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.

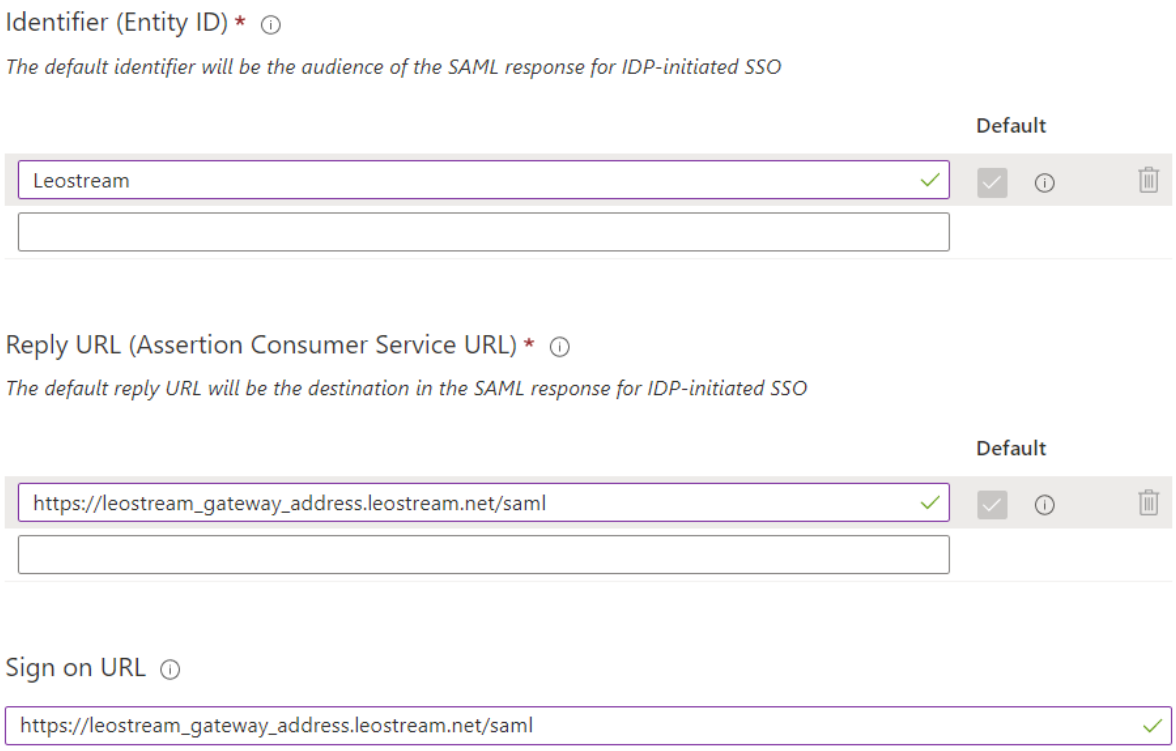


8. In the **Basic SAML Configuration** pane:

    a. Modify the Default Entity ID 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 Azure AD.

    b. Set the **Reply URL** and **Sign on URL** to direct Azure AD to your Leostream address with `/saml` 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 Azure AD.

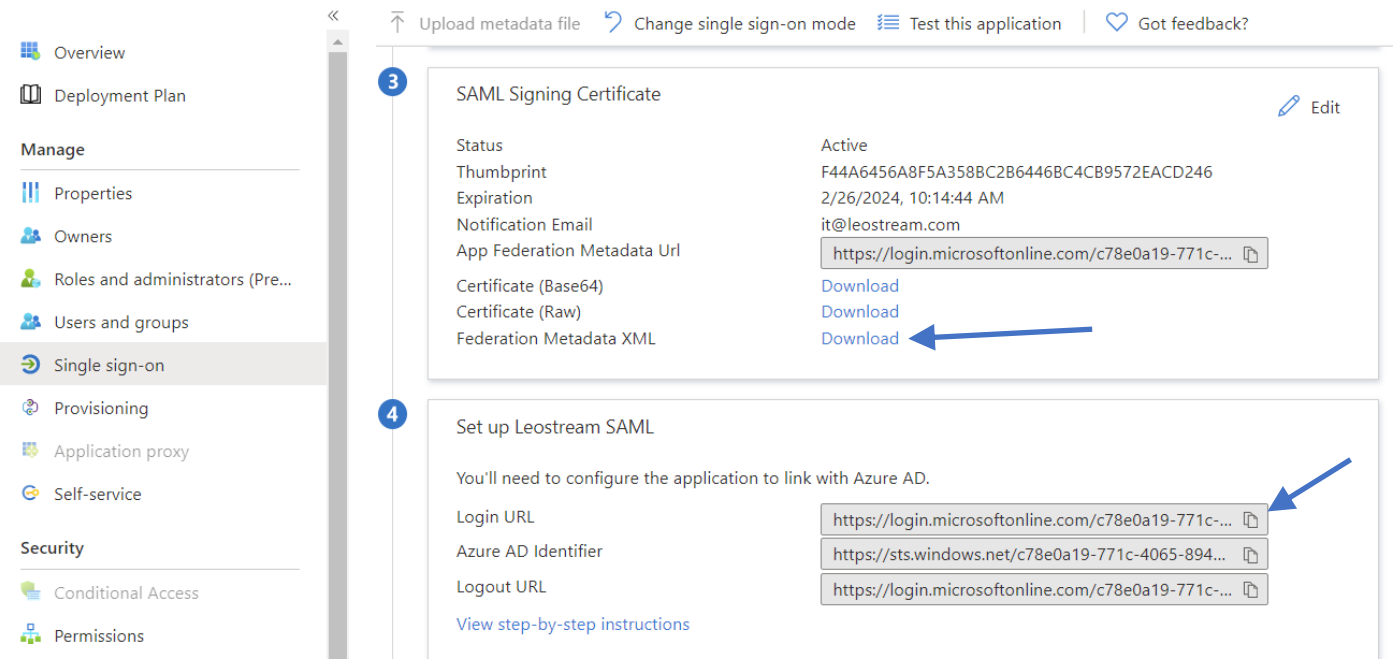
    The following figure shows an example Entity ID and Reply and Sign on URLs. In this example, the Leostream Sign on URL is the Leostream Gateway address. To determine how to set the Sign on URL for your environment, consult the "Determining your Leostream Single Sign-On URL" in the Leostream Guide for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



    c. 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.



Preparing Leostream to Work with Your Azure AD

After building your Enterprise Application in Azure, register it with Leostream 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 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.

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 Leostream for more information.

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

Final Configuration steps in Azure-AD

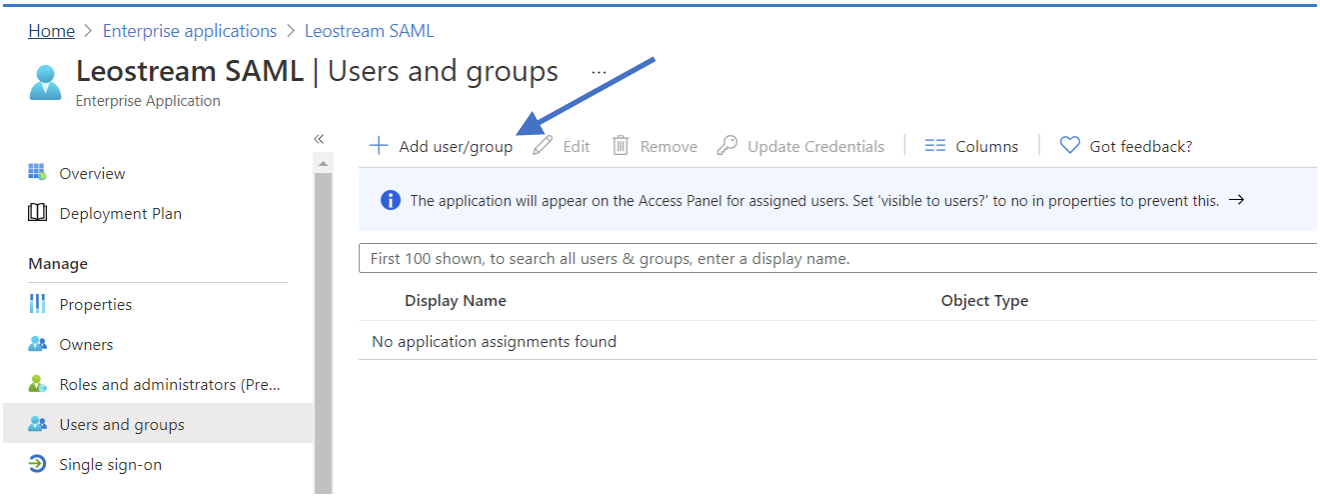
After saving your SAML authentication server in Leostream, return to your Azure portal to indicate which users may access the Enterprise Application created for your Leostream environment.

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

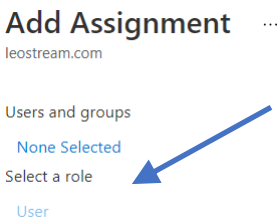
2. Select your Leostream Enterprise Application from the **All applications** list.

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 Azure AD 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.

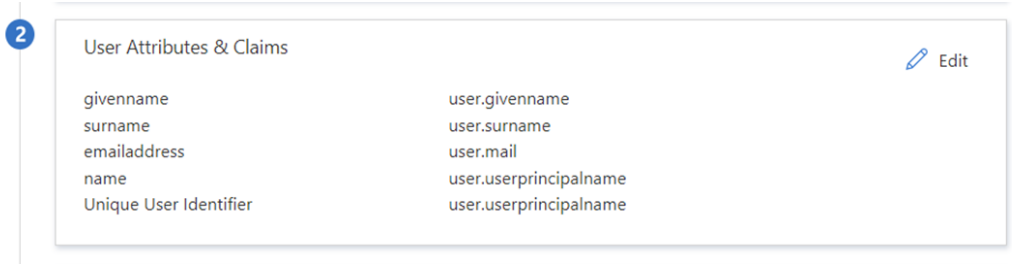
By default, Azure AD does not share group data via the SAML assertion sent to Leostream. To assign Leostream policies based on group membership, you must alter the **User Attributes & Claims** section of your Leostream Enterprise Application.

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**.

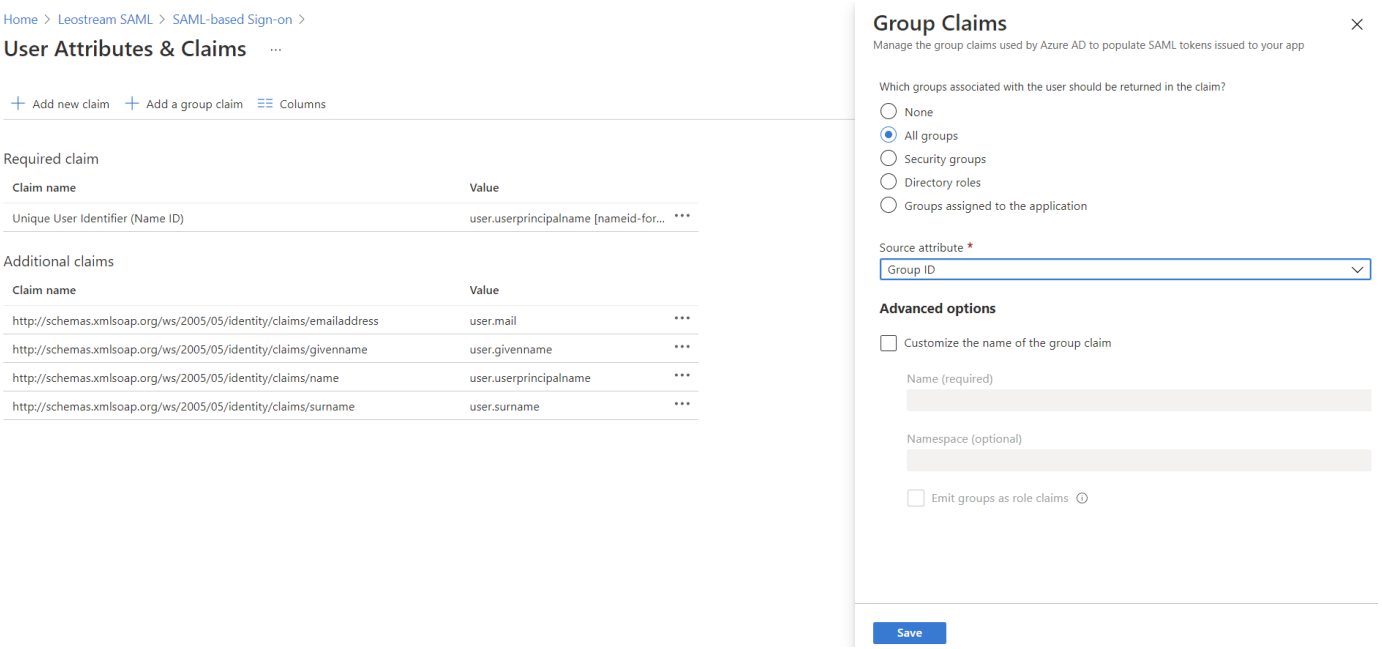
4. Click the **Edit** link in section **2. User Attributes & Claims**, shown in the following figure, to add group claims to the SAML assertion.



5. In the **User Attributes & Claims** pane, click **Add a group claim**.

6. In the **Group Claims** pane, select **All groups** to send all of the user's groups to Leostream

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 Leostream.

Assigning Policies for Azure AD Logins

When you have an active Azure AD 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 Azure AD 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 Azure AD. You configure your assignment rules, as follows.

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

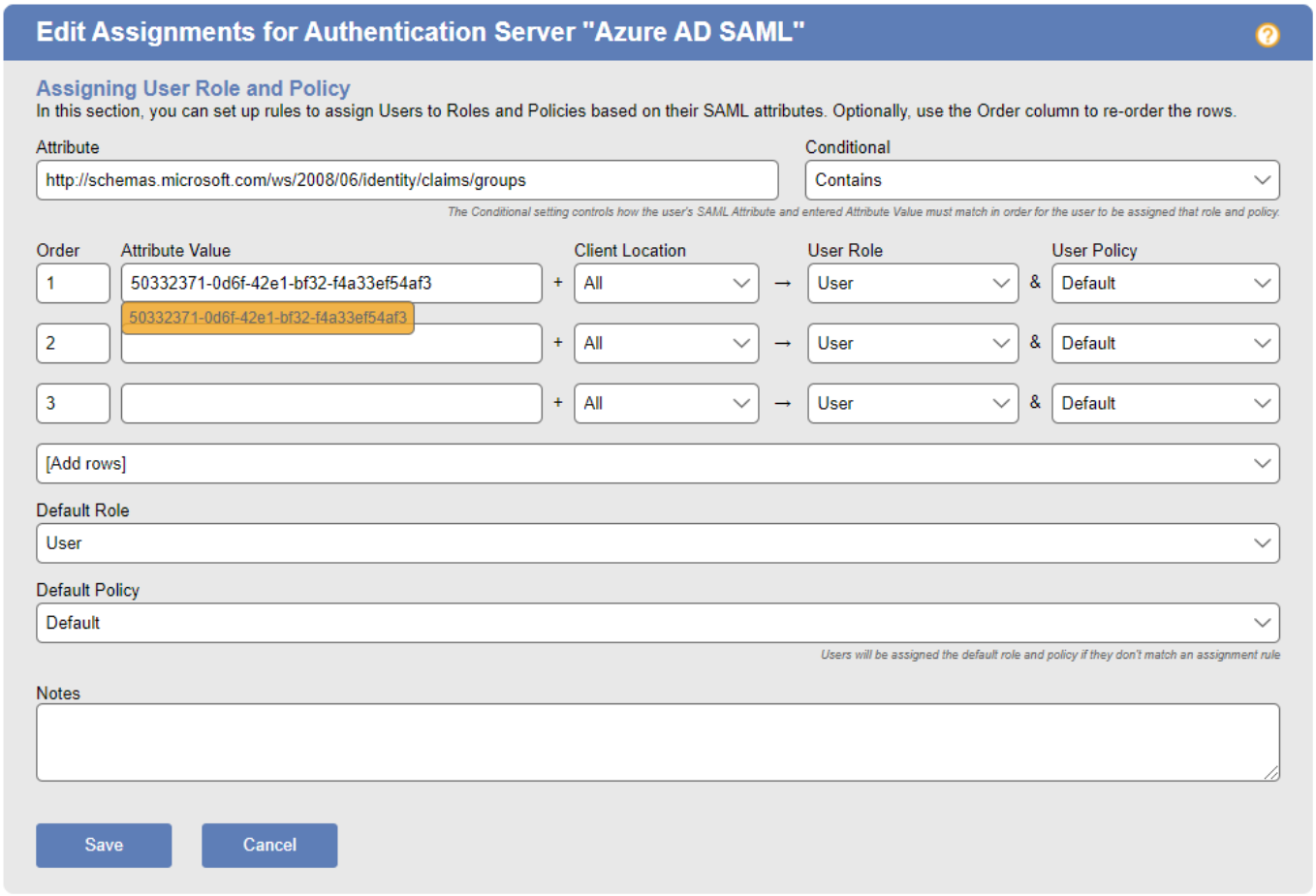
2. Click **Edit** on your Azure AD Authentication Server.

3. Enter the specific attribute Leostream uses for policy assignments in the **Attribute** edit field. For Azure AD, the attribute is the full URL claim name shown in the **User Attributes & Claims** pane. For example, to use the Azure AD 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
   ```

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

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



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 Azure AD, 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 Azure AD SAML Logins

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

1. In your Azure portal, go to **> All services > Azure AD 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 and groups** header to select the users/groups that are required to use MFA.

4. Below the **Cloud apps or actions** 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 Azure MFA 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.