Configure SAML Remote Authentication for Silver Peak Unity Orchestrator with Microsoft Azure AD

Silver Peak Unity Orchestrator supports remote authentication via Security Assertion Markup Language (SAML). This document provides information about how to enable Orchestrator Single Sign-On (SSO) using the SAML 2.0 framework in Azure Active Directory (Azure AD).

SAML remote authentication is only supported in Orchestrator 9.0.0 and higher.

It may be helpful to use a browser extension, such as SAML-tracer, to help in troubleshooting any issues you may have while configuring SAML SSO.

Overview

You can grant users access to Orchestrator by using Azure AD as your Identity Provider (IdP), configuring SAML-based SSO, and adding the configuration to a new remote authentication server in Orchestrator. This document contains the following sections to help you configure SAML-based SSO in Azure AD for remote authentication in Orchestrator:

Log in to Azure

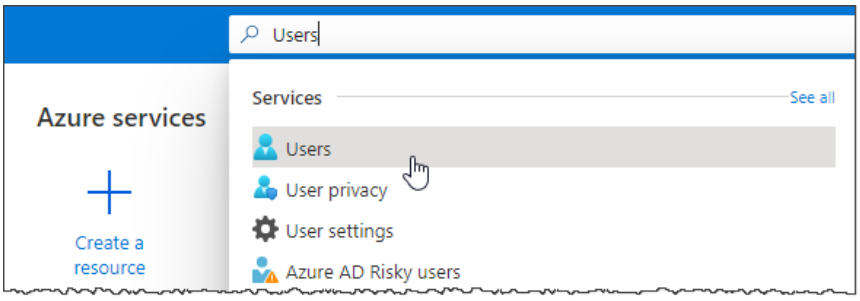
To get started, log in to the Azure Portal and switch to the directory that you will use to manage users, groups, and applications.

Before going any further, ensure that you have sufficient privileges to create an Enterprise Application and configure SAML SSO in Azure AD.

Add Users to Azure AD

You don't need to create local users in Orchestrator when using remote authentication, but your users must be authenticated with Azure before they can be logged in to Orchestrator.

1. In the Azure Portal, go to the Users page.



2. If you need to add any users, click **+ New user** at the top of the user table, or import users in bulk via CSV.

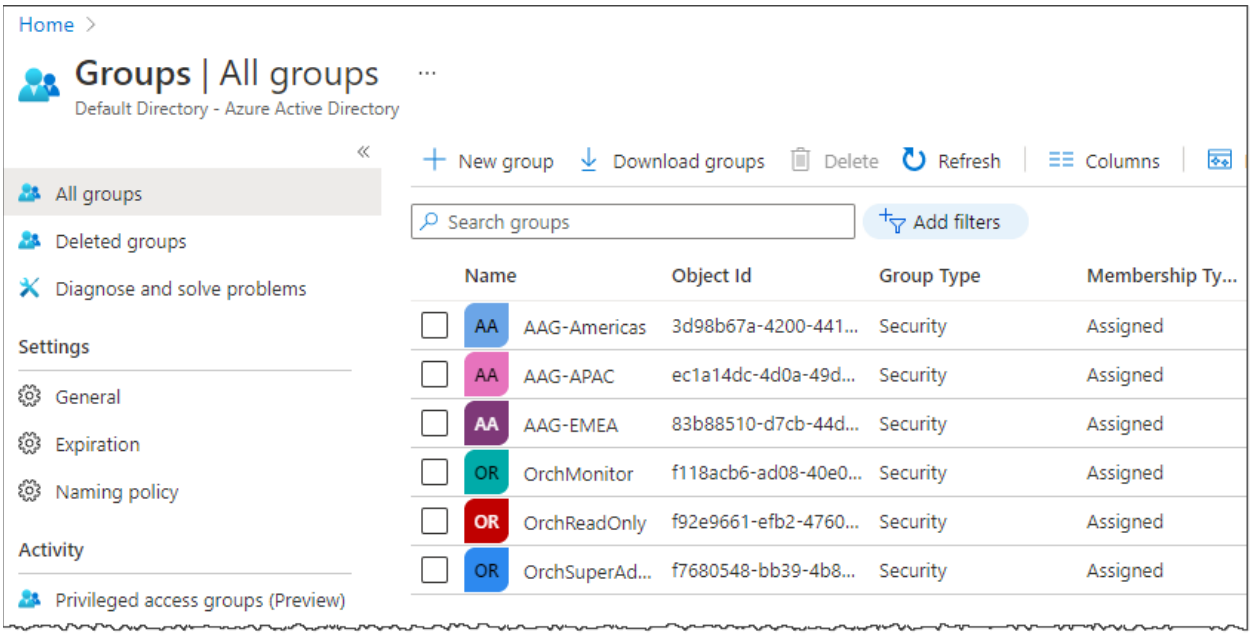
   All users must be assigned at least one administrative role in Azure. For Orchestrator authentication, the specific role does not matter. See this page for more information.

Configure Azure AD Groups

SAML remote authentication supports role-based access control (RBAC) and appliance access groups (AAG), which are sent as optional claims from Azure to Orchestrator. You can manage RBAC and AAG membership in Orchestrator with groups in Azure. For each RBAC or AAG role you want to assign through SAML logins, you will need a group in Azure.

If you configure the AAG attribute on the Orchestrator remote authentication server (see Configure SAML Authentication in Orchestrator), you must ensure that all users belong to one of the appliance access groups. You cannot grant access to all appliances by not sending the claim. Instead, you would have to create a group in Azure that maps to an Orchestrator AAG for all appliances.

In the example image below, six groups have been created for passing three AAGs and three RBAC roles via SAML.



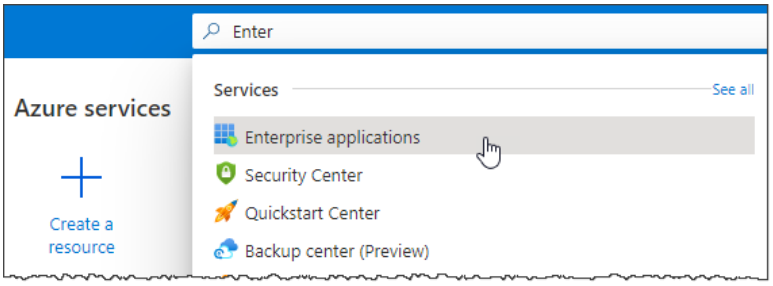
After you have created all the groups you need, add users to the groups according to the roles and appliance access you want them to have in Orchestrator. See this page for more information.

Orchestrator users should only have one RBAC role and one AAG assigned, so be sure that Azure users are not members of more than one of each group type.

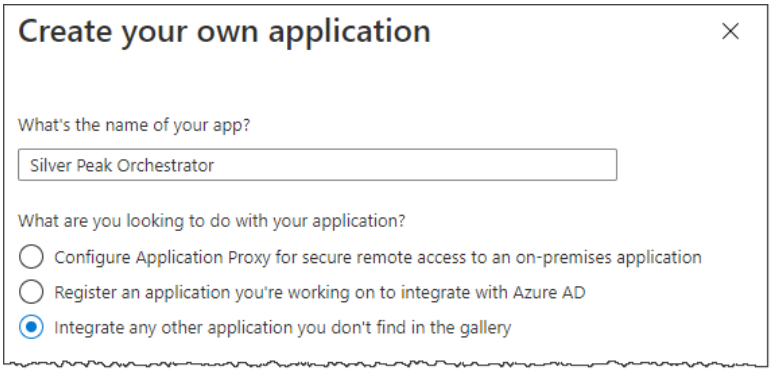
Create an Enterprise Application with SAML-based SSO

After organizing users and groups, you are ready to configure SAML-based SSO in an Enterprise Application.

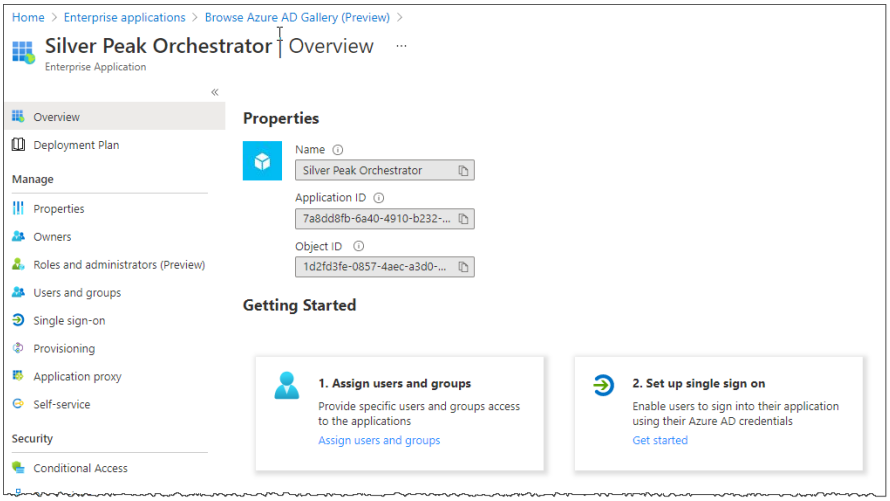
1. In the Azure Portal, go to the Enterprise Applications page.



2. At the top of the applications table, click **+ New application**.
3. In the application gallery, click **+ Create your own application**.
4. In the details panel, enter a name for the application, select the “Integrate any other application you don't find in the gallery” option, and then click **Create**.

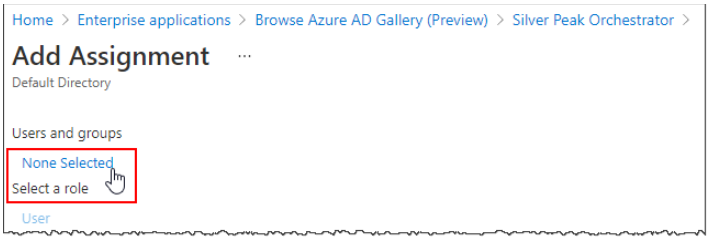


When ready, the home page for the new application appears.

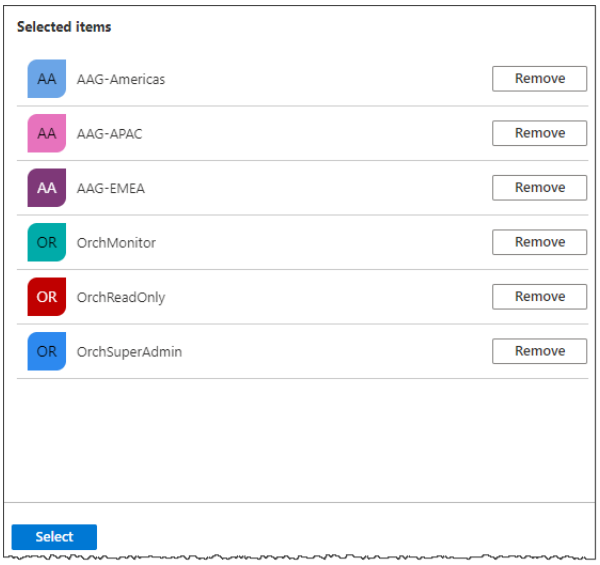


5. In the menu on the left, click **Users and groups** under Manage.

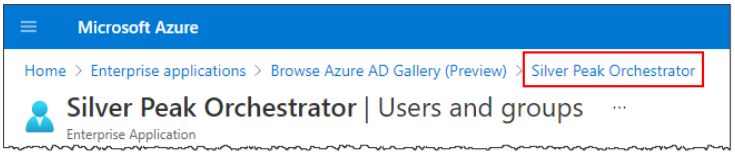
6. On the Users and groups page, click **+ Add user/group**.
7. On the Add Assignment page, click **None Selected** under Users and groups.



8. In the panel to the right, select each of the role and AAG groups that you created earlier, then click **Select**.



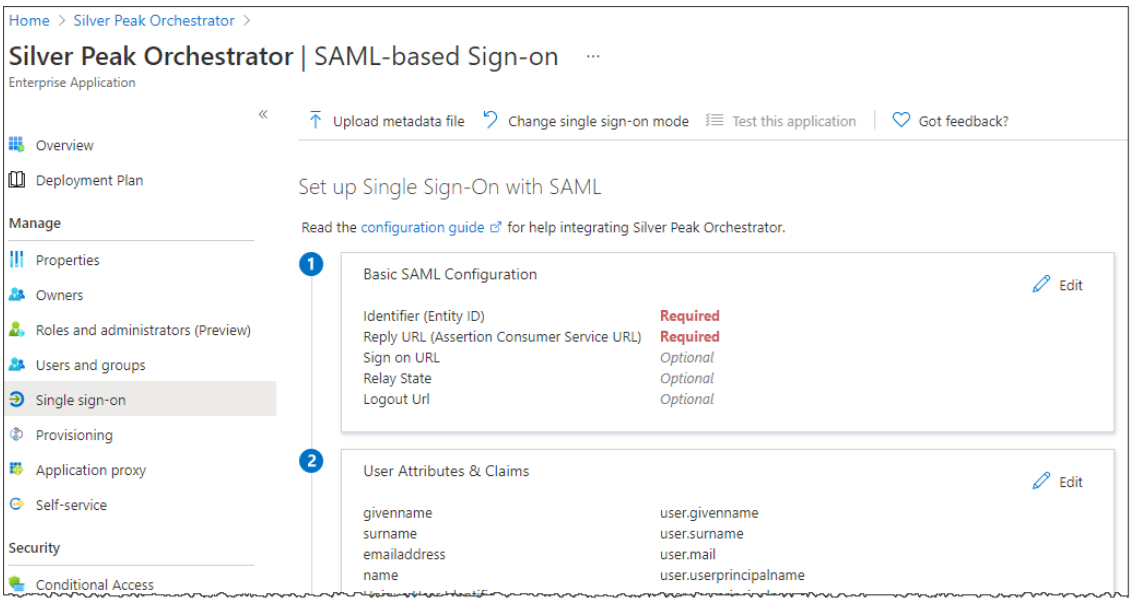
9. Back on the Add Assignment page, click **Assign**.
10. Click the application name in the breadcrumbs at the top of the page to return to the application home page.



11. In the menu on the left, click **Single sign-on** under Manage.
12. On the Single sign-on page, click **SAML** as the sign-on method.

The SAML-based sign-on summary is displayed for your application.

You will use details from this page to configure remote authentication in Orchestrator.



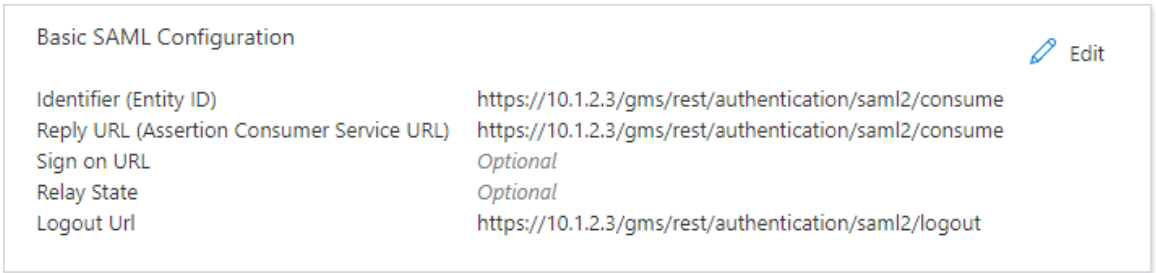
SAML Configuration

After creating the application and selecting SAML as the sign-on method, you will need to add some details based on the IP address or hostname of your Orchestrator server.

1. On the SAML-based Sign-on page, click **Edit** in the Basic SAML Configuration box.
2. In the panel to the right, fill in the following values:

Field	Value
Identifier (Entity ID)	https://<*orch_ip_or_hostname*>/gms/rest/authentication/saml2/consume
Reply URL	https://<*orch_ip_or_hostname*>/gms/rest/authentication/saml2/consume
Logout URL	https://<*orch_ip_or_hostname*>/gms/rest/authentication/saml2/logout

3. Delete the default Identifier (Entity ID) that was pre-populated in the panel (click).
4. At the top of the panel, click **Save**.
5. When the configuration has been saved, click **X** to close the Basic SAML Configuration panel.

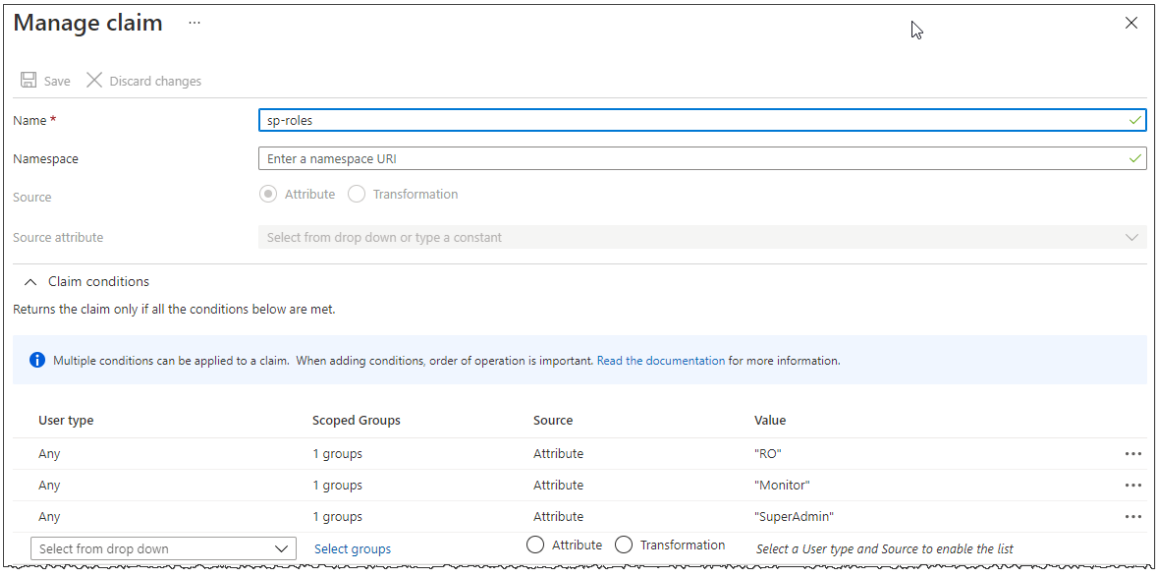


Add Claims for RBAC and AAG

Follow the steps in this section to configure the claims that map users to RBAC roles and AAGs according to their Azure group membership.

1. On the SAML-based Sign-on page, click **Edit** in the User Attributes & Claims box.
2. On the User Attributes & Claims page, click **+ Add new claim**.

3. For the RBAC claims, enter **sp-roles** for the claim name.
4. Click **Claim conditions** to expand it.
5. For each Azure group that maps to an RBAC role, add a condition for **Any** user type, select the scoped group that corresponds to the selected role, select **Attribute** as the source, and type in the exact name of the Orchestrator role in the Value field.
6. Click **Save**.



> Ensure that users are only members of one “role” group in Azure.

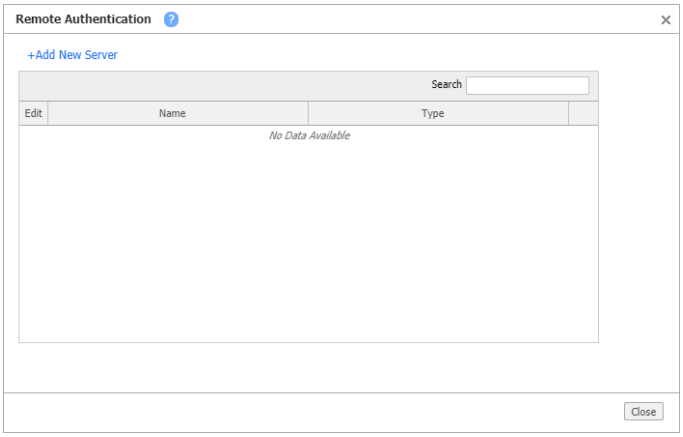
7. Repeat steps 3-6 above, using **sp-aag** as the claim name and mapping the appliance groups in Azure to the named appliance groups in Orchestrator.

> Ensure that users are only members of one “appliance” group in Azure.

Configure SAML Authentication in Orchestrator

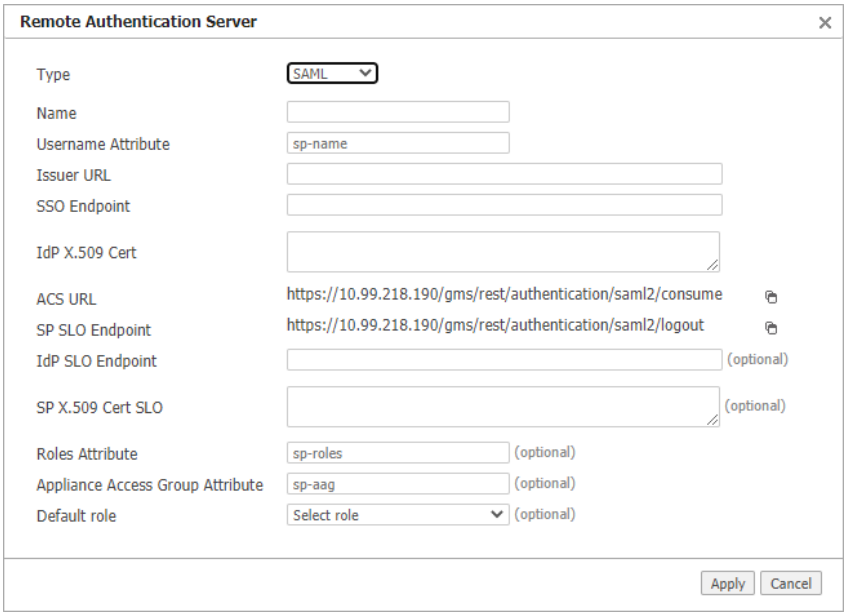
1. Log in to Orchestrator as an administrative (read-write) user.
2. Click **Orchestrator > Orchestrator Server > Users & Authentication > Authentication**.

   The Remote Authentication dialog appears.



3. Click **+Add New Server**.

   The Remote Authentication Server dialog appears.



4. For Type, select **SAML** and fill in the available fields for the new server, as follows:

   Only the required fields are described below. Any other fields are optional and do not need to be modified for this configuration.

Field	Value
Name	Enter a name to identify the server. This name will be displayed in a button on the Orchestrator login page as an alternate authentication method.
Username Attribute	This should be the full Attribute Name sent by Azure AD. In our case, it is http://schemas.microsoft.com/identity/claims/displayname
Issuer URL	This is the **Azure AD Identifier** value for the application, found in box 4 on the summary page (see image at top of page 6).
SSO Endpoint	This is the **User access URL** from the application properties. Click **Properties** on the application summary page (see image at top of page 6).
IdP X.509 Cert	This is the Base64 certificate, found in box 3 on the summary page (see image at top of page 6). Click the **Download** link next to Certificate (Base64), open the downloaded .cer file in a text editor, then paste the entire contents into this field.
Roles Attribute	This is the name given to the RBAC claim in Azure: **sp-roles**
Appliance Access Group Attribute	The is the name given to the AAG claim in Azure: **sp-aag**
Default role	If you want to set a default role for any users who do not match the conditions of the RBAC claim, you can set it here.

5. Click **Apply**, then click **Close** in the Remote Authentication dialog.

   Your Orchestrator login screen will now display a button that users can click to log in using the new SAML method.

Revision History

Mar 2, 2021 Rev A: Initial document revision.