SAML Remote Authentication for Aruba Orchestrator

USING MICROSOFT AZURE ACTIVE DIRECTORY

October 2022
TABLE OF CONTENTS

INTRODUCTION ........................................................................................................................................... 3
SUMMARY .................................................................................................................................................... 3
ADDING USERS AND CREATING GROUPS IN AZURE AD ...................................................................... 3
   ADDING USERS TO AZURE AD............................................................................................................. 3
   CREATING GROUPS AND ASSIGNING USERS TO GROUPS. ............................................................. 4
ADDING ORCHESTRATOR AS AN ENTERPRISE APPLICATION IN AZURE AD .................................... 6
   CREATING AN ENTERPRISE APPLICATION ........................................................................................ 6
   ADDING USERS TO THE NEW ENTERPRISE APPLICATION ............................................................. 6
   ADDING SAML AUTHENTICATION TO ORCHESTRATOR ............................................................... 7
   Section 1 : Basic SAML Configuration ............................................................................................... 9
   Section 2: Attributes & Claims ............................................................................................................ 9
   Section 3: SAML Signing Certificate ................................................................................................. 10
   Section 4: Set up [enterprise application name] .............................................................................. 10
CONFIGURE SAML REMOTE AUTHENTICATION IN ORCHESTRATOR ................................................. 11
MAPPING AZURE AD GROUPS TO ORCHESTRATOR RBAC ROLES .................................................... 12
   AZURE CONFIGURATION STEPS ..................................................................................................... 13
   ORCHESTRATOR CONFIGURATION STEPS .................................................................................. 14
MAPPING MULTIPLE ROLES .................................................................................................................... 15
INTRODUCTION
This document describes how to configure remote authentication for Orchestrator using single sign-on (SSO), and how to configure security assertion markup language (SAML) and use it to authenticate users who access Orchestrator.

SUMMARY
To grant users access to Orchestrator via SAML, you need to complete the following items:
- Add users and create groups in Microsoft® Azure® Active Directory® (AD).
- Add Orchestrator as an Enterprise application with SAML authentication in Azure.
- Configure SAML remote authentication in Orchestrator.

ADDING USERS AND CREATING GROUPS IN AZURE AD
To add users and create groups in Azure AD, you need to have an Azure account. If you don’t have an account, you can set up a free trial account at https://portal.azure.com/.

Note: Because the goal is to authenticate users via Azure AD, you do not need to create a local user in Orchestrator.

Adding Users to Azure AD
You must add users to Azure AD before you create groups.
1. Log into Azure portal and type “Azure Active Directory” in the search field.
2. When you are in the Active Directory, in the left pane click Users, and then click + Add to add a new user.

![Adding Users to Azure AD](image)

3. On the screen that opens, complete the following fields:
   - **User name**: Enter a username for the user.
   - **Name**: Enter a name for the user.
   - **Password**: Enter a strong password for the user.
4. Click **Create** to create the new user.
5. To add more users, repeat steps 1-4 for each user.

Creating Groups and Assigning Users to Groups

After you have added users, you need to create a group(s) so you can assign the users to a group. This is an important step because SAML supports role-based access control (RBAC).

1. In the left pane, click **Groups**. You can either add a new group or assign the user to an existing group.
2. To create a new group, click **New group**.
The New Group dialog box opens.

3. Complete the following fields:
   - **Group type**: Select **Security** from the drop-down menu.
   - **Group name**: Enter a name for the group.

4. Click **Create** to create the new group.

After the group is created, you can assign users to the group. To add users, in the left pane click **Members**, and then click **+ Add members**. Search for a user(s) by username in the Add members window, and then click the username in the list to add the user to the group.
ADDING ORCHESTRATOR AS AN ENTERPRISE APPLICATION IN AZURE AD

After adding users and creating groups, you must add Orchestrator as an enterprise application in Azure AD.

Creating an Enterprise Application

1. Type “Enterprise applications” in the search field.
2. When the tab opens, click + New application.

3. At the top of the application table, click + Create your own application.

Adding Users to the New Enterprise Application

You need to add users to the new enterprise application you created in Azure.

1. In Azure, click the new enterprise application you created for Orchestrator. The Overview page for the new enterprise application opens.
2. In the left pane, click Users and groups.

3. In the Users window, search for a user(s) by username.
4. Click Create to add the user to the enterprise application, and then click the username in the list to add the user to the enterprise application.

5. Click Assign when you are done adding users.

*Note: Make sure that you click Assign on the bottom left of the screen after adding users or the users will not be added to the enterprise application.*

6. Click the enterprise application name at the top of the page to return to the enterprise application Overview page.

---

**Adding SAML Authentication to Orchestrator**

From the enterprise application Overview page, you must add SAML authentication to Orchestrator. In the left pane, click **Single sign-on**.

The enterprise application SAML-based Sign-on page opens. The page contains five sections for SAML configuration. You will only work with the first four sections. There is information that you will copy from this page to Orchestrator and from Orchestrator back to this SAML SSO configuration page in Azure. The following information describes the fields that need to be completed in each section.
Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Aruba Orch.

1. Basic SAML Configuration
   - Identifier (Entity ID): https://192.168.1.150/gmc/rest/authentication/saml2/consume
   - Sign on URL: Optional
   - Relay State (Optional): Optional
   - Logout URL (Optional): https://192.168.1.150/gmc/rest/authentication/saml2/logout

2. Attributes & Claims
   - givenname: user.givenname
   - surname: user.surname
   - emailaddress: user.email
   - name: user.principalname
   - Unique User Identifier: user.principalname

3. SAML Signing Certificate
   - Status: Active
   - Thumbprint: 9B1F6A5D64C133C1D608116D16F80A650A61607
   - Expiration: 2/1/2023, 05:40:00 AM
   - App Federation Metadata URL: https://login.microsoftonline.com/052eaf703-f6b...
   - Certificate (Base64): Download
   - Certificate (Pfx): Download
   - Federation Metadata XML: Download

4. Setup Aruba Orch
   - Login URL: https://login.microsoftonline.com/052eaf703-f6b...
   - Azure AD Identifier: https://sts.windows.net/052eaf703-f6b-
   - Logout URL: https://login.microsoftonline.com/052eaf703-f6b...
   - View step-by-step instructions

5. Test single sign-on with Aruba Orch
   - Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.
   - Test
Section 1: Basic SAML Configuration
The following table describes the correlation of Azure and Orchestrator fields. To edit these fields in Azure, click the ellipse (…) in the Basic SAML Configuration section.

<table>
<thead>
<tr>
<th>Azure</th>
<th>Orchestrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier (Entity ID)</td>
<td>ACS URL from Orchestrator</td>
</tr>
<tr>
<td>Reply URL (ACS URL)</td>
<td>ACS URL from Orchestrator</td>
</tr>
<tr>
<td>Logout URL</td>
<td>SP SLO endpoint from Orchestrator</td>
</tr>
</tbody>
</table>

- “Identifier (Entity ID)” and “Reply URL (Assertion Consumer Service URL)” = ACS URL from Orchestrator
  - “https://<Orch IP or Hostname>/gms/rest/authentication/saml2/consume”

- “Logout URL” = SP SLO Endpoint from Orchestrator
  - “https://<Orch IP or Hostname>/gms/rest/authentication/saml2/logout”

Section 2: Attributes & Claims
In the Attributes & Claims section, click the ellipse (…) and copy the highlighted line, and then paste it into a text editor such as Notepad. You will paste this information into the Username Attribute field when you configure SAML authentication in Orchestrator.

```
Required claim
Claim name: Unique User Identifier (Name ID)
Value: user\userprincipalname (nameid-for... ***

Additional claims
Claim name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Value: user\email ***

Claim name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Value: user\givenname ***

Claim name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Value: user\userprincipalname ***

Claim name: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Value: user\surname ***
```
Section 3: SAML Signing Certificate
Click SAML-based Sign-on at the top of the page to return to the SAML-based Sign-on page for the enterprise application. In the SAML Signing Certificate section, there are three certificates available. Download the highlighted certificate (Base64) and open it using a text editor such as Notepad. You will paste this information into the IdP X.509 Cert field when you configure SAML authentication in Orchestrator.

![SAML Signing Certificate Table](image)

Section 4: Set up [enterprise application name]
Click SAML-based Sign-on at the top of the page to return to the SAML-based Sign-on page for the enterprise application. In the Set up [enterprise application name] section, click the copy icon next to Azure AD Identifier and paste it into a text editor such as Notepad. You will paste this information into the Issuer URL field when you configure SAML authentication in Orchestrator.

![Set up Aruba Orch](image)
CONFIGURE SAML REMOTE AUTHENTICATION IN ORCHESTRATOR

To complete the SAML authentication process, you need to add SAML authentication to Orchestrator at Orchestrator > Orchestrator Server > Users & Authentication > Authentication.

1. Click **Add New Server**.
2. Select **SAML** from the **Type** field, and then complete the following fields:
   - **Name**: Enter a name for the server.
   - **Username Attribute**: Paste the information that you copied from the Attributes & Claims section (section 2) of the SAML-based Sign-on page in Azure into this field.
   - **Issuer URL**: Paste the information that you copied from the Set up [enterprise application name] section (section 4) of the SAML-based Sign-on page in Azure into this field.
   - **SSO Endpoint**: Copy this information from the User access URL field in Azure. To access this information in Azure, click **Enterprise applications**, then click the name you assigned to Orchestrator, and from the left pane click **Properties**.
     - **Idp X.509 Cert**: Paste the information that you copied from the SAML Signing Certificate section (section 3) of the SAML-based Sign-on page in Azure into this field.
   - **Default Role**: This is needed if you did not define RBAC in the user attributes in the Attributes & Claims section (section 2) of the SAML-based Sign-on page in Azure. Select the role that best suits the needs of your organization.
3. Click **Apply** to save your changes.

After all the changes are applied, Orchestrator displays a new login button for Azure SAML configuration. Use your Azure AD credentials to log in to Orchestrator.

**MAPPING AZURE AD GROUPS TO ORCHESTRATOR RBAC ROLES**

We recommend that you define roles in Azure that map to Orchestrator role-based access control (RBAC). This is helpful for creating different permission levels for different user accounts. The following figure shows the setup for RBAC in Orchestrator that you can map to the Azure AD groups.
**Azure Configuration Steps**

1. In Azure AD, click **Enterprise applications**, then click the name you assigned to Orchestrator, and from the left pane click **Single sign-on**.
   
The SAML-based Sign-on page opens.

2. In section 2 User Attributes & Claims click **Edit** and then click **+ Add new claim**.

3. In the Manage claim section, complete the following fields:
   - **Name**: Enter a name for the claim.
   - **Source**: Click the **Attribute** radio button.
   - **Expand Claim conditions** and complete the following:
     - **User type**: Select **Members**.
     - **Scoped Groups**: Click **Select groups** and select the group that you created in Azure AD.
     - **Source**: Click the **Attribute** radio button.
     - **Value**: Enter based on Orchestrator RBAC set up.
Orchestrator Configuration Steps

2. Click the edit icon to the left of the server you created.
3. In the Roles Attribute field, enter the claim name you created in the Azure Configuration Steps section. The following example uses "sp-roles."

![Remote Authentication Server](image-url)
MAPPING MULTIPLE ROLES

There might be situations when a user needs to have multiple roles assigned to them. For example, when an RBAC role needs read access to all the Orchestrator menus but only needs read-write access to a subset of administrative tasks.

To accomplish this, add the user to multiple groups and assign each group one or more attributes that map to a role in Orchestrator.

1. In Azure AD, click **Enterprise applications**, then click the name you assigned to Orchestrator, and from the left pane click **Single sign-on**.

   The SAML-based Sign-on page opens.

2. In section 2 **User Attributes & Claims** click **Edit** and edit an existing claim or create a new claim.

3. In the Manage claim section, expand **Claim conditions** and complete the following:

   - **User type**: Select **Members**.
   - **Scoped Groups**: Click **Select groups** and select a group to which the user is assigned.
   - **Source**: Click the **Attribute** radio button.
   - **Value**: Enter the name of the RBAC role that you want to assign to this group. This can be a pre-defined Orchestrator role, or it can be a custom role that you created in Orchestrator. When you add this value to the group, all users in this group will be granted the permissions in Orchestrator that are associated with this role.

   The following figure shows a claim that is passing multiple roles because it has multiple groups. Each group has an assigned attribute (shown in the Value column) that is mapped to a role in Orchestrator.

![Manage Claim](image-url)

   The following figure shows a claim that is passing multiple roles because it has multiple groups. Each group has an assigned attribute (shown in the Value column) that is mapped to a role in Orchestrator.

<table>
<thead>
<tr>
<th>User type</th>
<th>Scoped Groups</th>
<th>Source</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members</td>
<td>1 groups</td>
<td>Attribute</td>
<td>“NS_Monitor”</td>
</tr>
<tr>
<td>Members</td>
<td>1 groups</td>
<td>Attribute</td>
<td>“NS_Support_Read”</td>
</tr>
<tr>
<td>Members</td>
<td>1 groups</td>
<td>Attribute</td>
<td>“NS_Support_Write”</td>
</tr>
</tbody>
</table>

**Note:** Place the group with the lowest privilege at the top of the Claim conditions table and place the group with the highest privilege at the bottom. This ensures that the role with the highest privilege is inherited when a user is part of more than one group.

To assign multiple roles to a group, add multiple attribute values in the Value column. Each value must be separated by a comma. In the following figure, the group in the second row contains two values in the Value column: “NS_Monitor” and “NS_Support”. Users in that group will be granted the permissions for both roles in Orchestrator.
You can add as many roles to a group as needed, but they must be comma separated for the Orchestrator to interpret the individual roles.