

The Aruba logo is displayed in a bold, orange, lowercase sans-serif font. The background of the page features a dark blue gradient with a large white circular shape in the top right corner and a dark red curved shape on the left side. A series of horizontal lines in a dark red color runs vertically along the right edge of the page.

a Hewlett Packard
Enterprise company

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

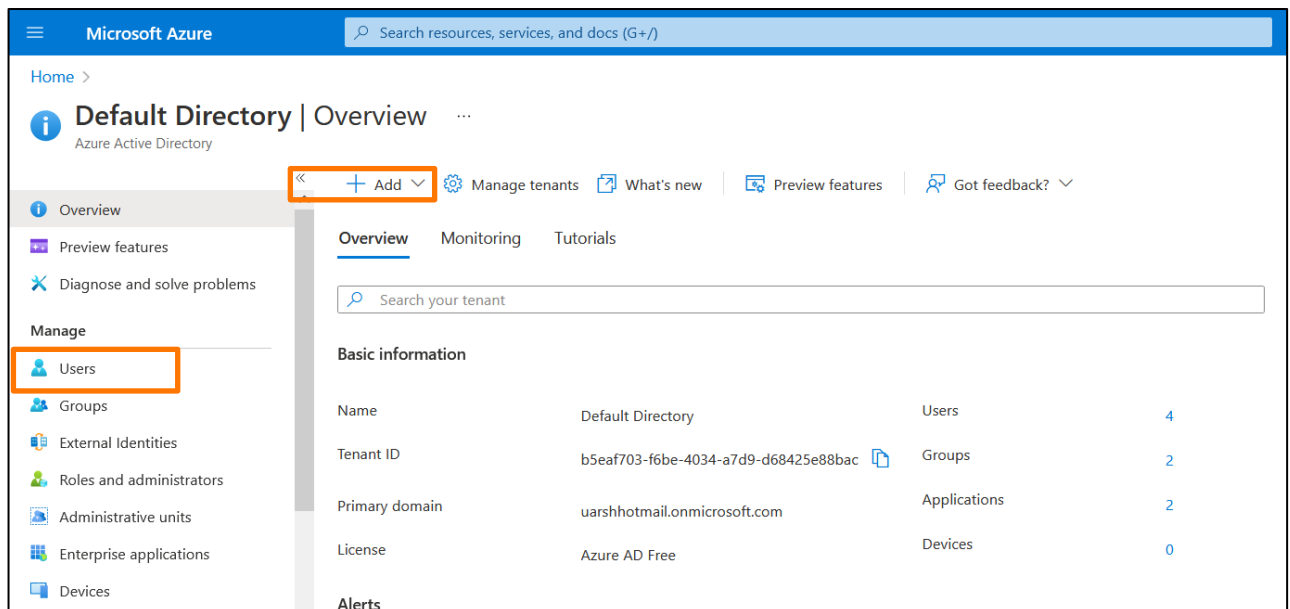
To add users and create groups in Azure AD, you need to have an Azure account. If you don't have an account, you can set up a free trial account at <https://portal.azure.com/>.

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.



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.

New user

Default Directory

[Got feedback?](#)

Create user

Create a new user in your organization. This user will have a user name like `alice@uarshotmail.onmicrosoft.com`.
[I want to create users in bulk](#)

Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * @ [The domain name I need isn't shown here](#)

Name *

First name

Last name

Password

Auto-generate password
 Let me create the password

Initial password

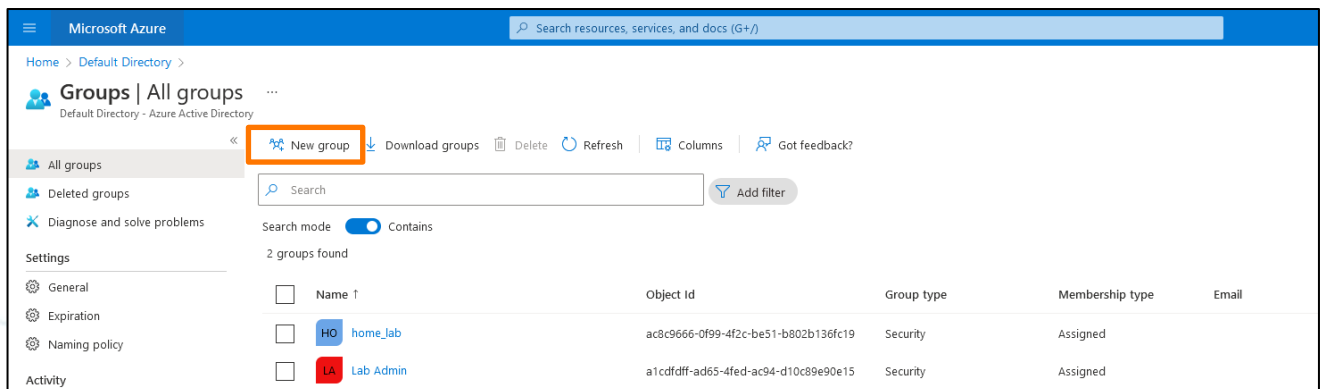
All the other settings are optional.

4. Click **Create** to create the new user.
5. To add more users, repeat steps 1-4 for each user.

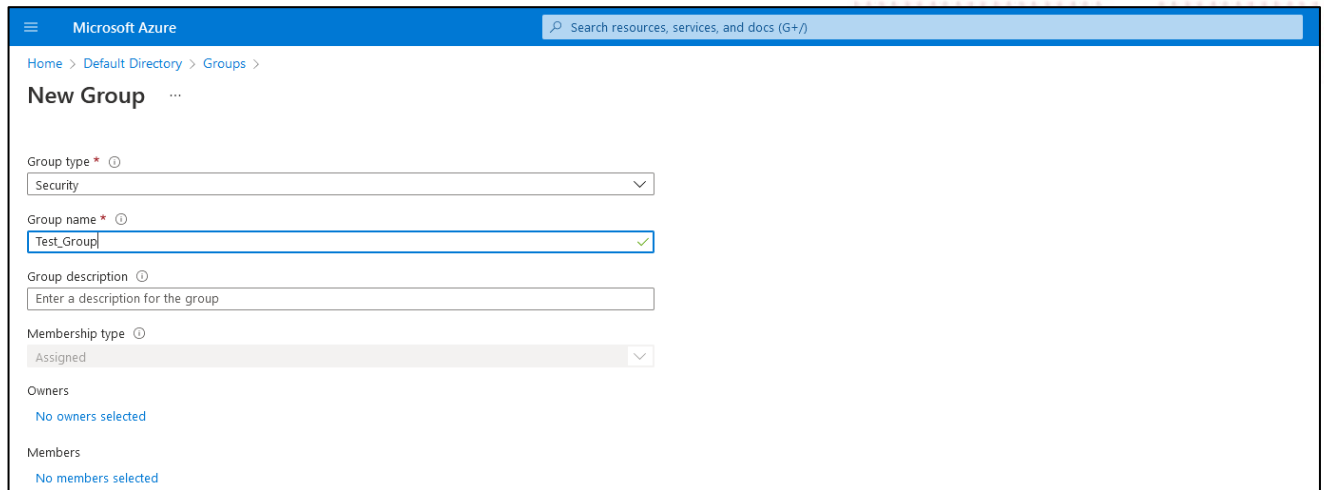
Creating Groups and Assigning Users to Groups

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.



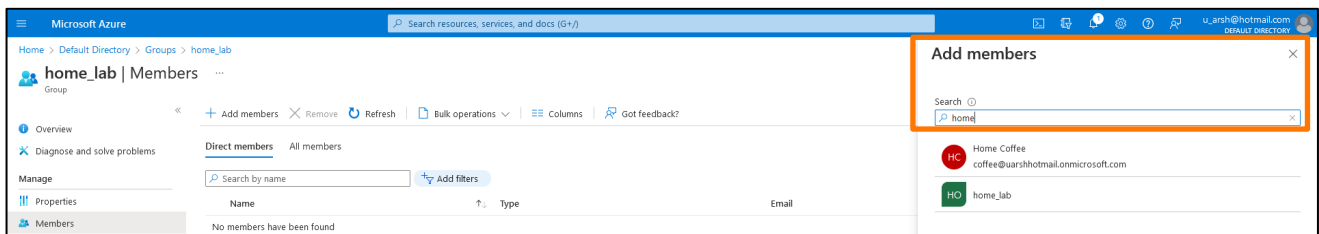
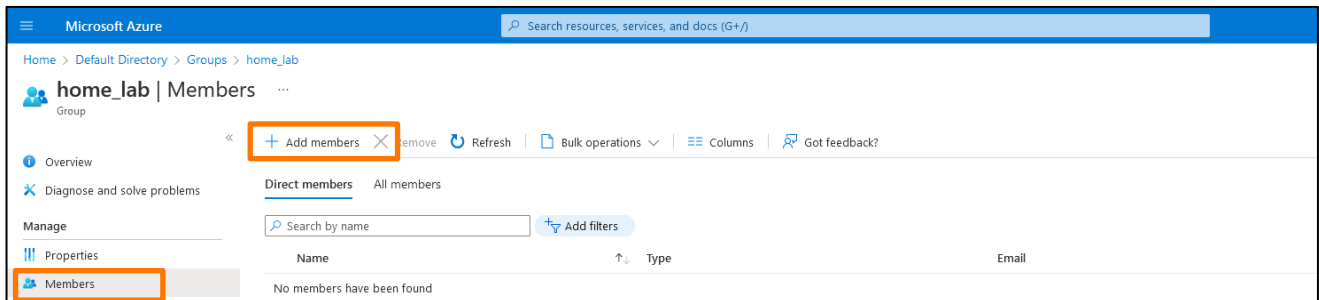
3. Complete the following fields:

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.

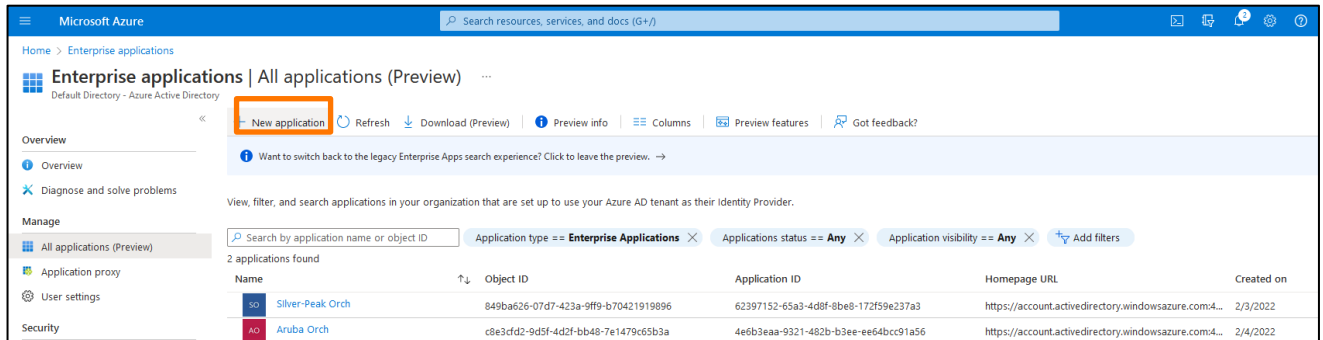


ADDING ORCHESTRATOR AS AN ENTERPRISE APPLICATION IN AZURE AD

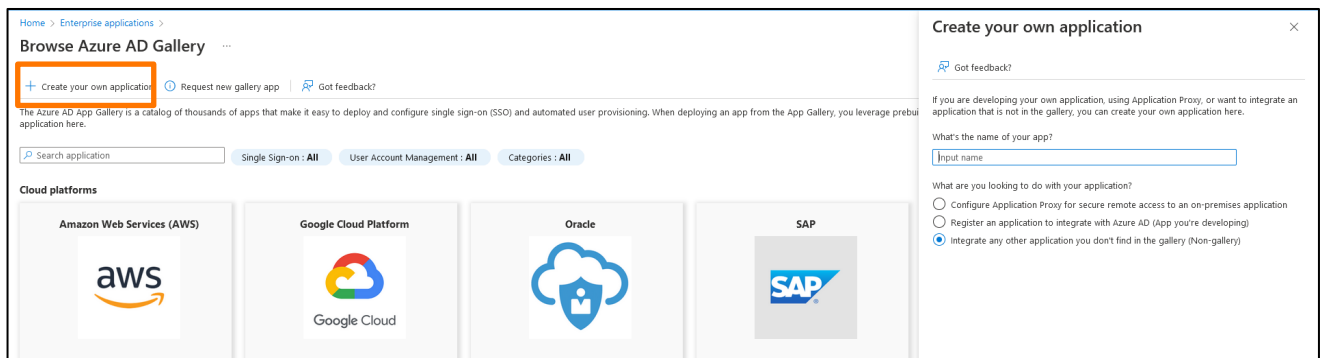
After adding users and creating groups, you must add Orchestrator as an enterprise application in Azure AD.

Creating an Enterprise Application

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



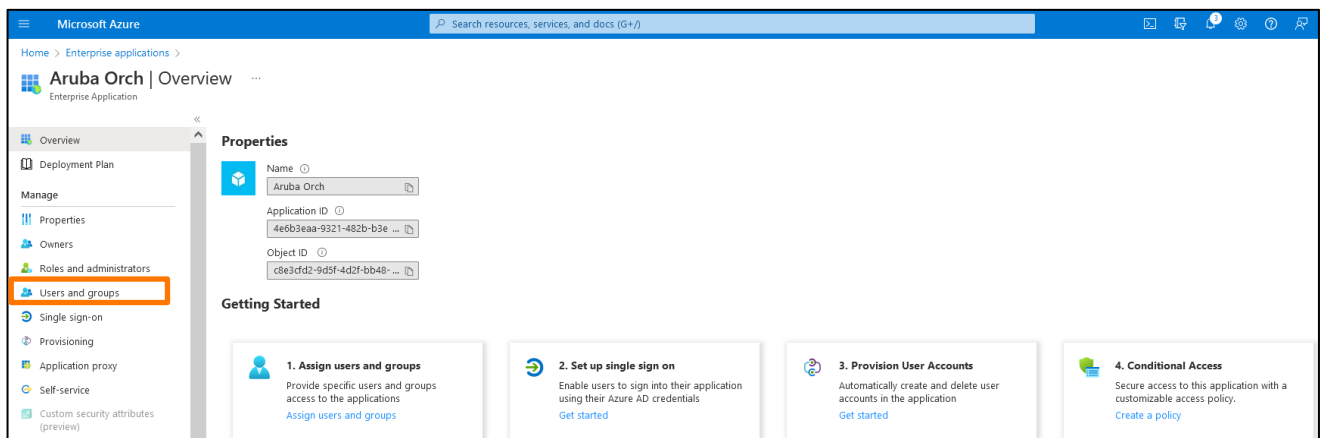
3. At the top of the application table, click **+ Create your own application**.



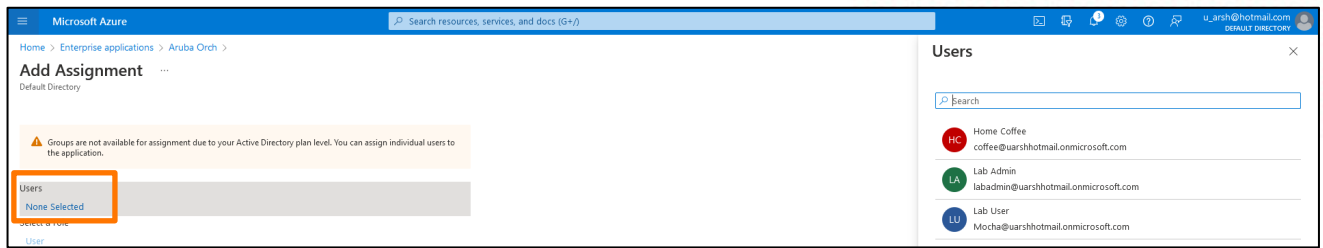
Adding Users to the New Enterprise Application

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**.



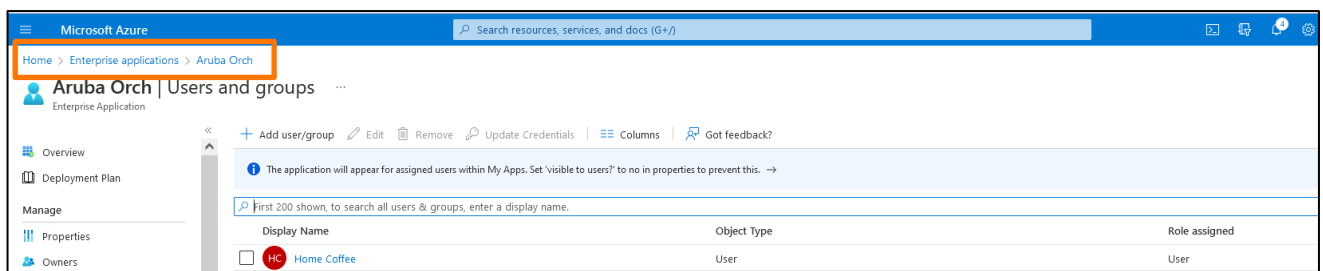
3. In the Users window, search for a user(s) by username.



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.

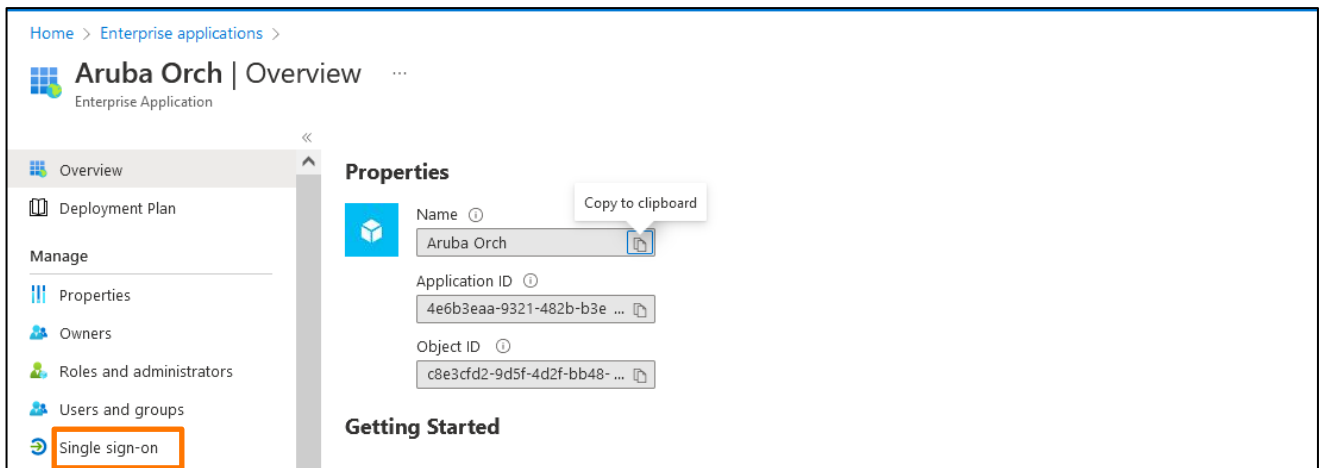
*Note: Make sure that you click **Assign** on the bottom left of the screen after adding users or the users will not be added to the enterprise application.*

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.

Aruba Orch | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)
- Security
- Conditional Access
- Permissions
- Token encryption
- Activity
- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Upload metadata file
Change single sign-on mode
Test this application
Got feedback?

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/gms/rest/authentication/saml2/consume
Reply URL (Assertion Consumer Service URL)	https://192.168.1.150/gms/rest/authentication/saml2/consume
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Uri (Optional)	https://192.168.1.150/gms/rest/authentication/saml2/logout

2
Attributes & Claims
...

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3
SAML Signing Certificate
...

Status	Active
Thumbprint	FAD4EFA9D35A24CD6E03811591498DAE59DA4807
Expiration	2/4/2025, 9:03:50 PM
Notification Email	u_arsh@hotmail.com
App Federation Metadata Uri	https://login.microsoftonline.com/b5eaf703-f6b...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4
Set up Aruba Orch

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/b5eaf703-f6b...
Azure AD Identifier	https://sts.windows.net/b5eaf703-f6b-4034-a...
Logout URL	https://login.microsoftonline.com/b5eaf703-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

8

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.

Azure	Orchestrator
Identifier (Entity ID)	ACS URL from Orchestrator
Reply URL (ACS URL)	ACS URL from Orchestrator
Logout URL	SP SLO endpoint from Orchestrator

- “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>”

1

Edit

Basic SAML Configuration	
Identifier (Entity ID)	https://192.168.1.150/gms/rest/authentication/saml2/consume
Reply URL (Assertion Consumer Service URL)	https://192.168.1.150/gms/rest/authentication/saml2/consume
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	https://192.168.1.150/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.

Home > Enterprise applications > Aruba Orch > SAML-based Sign-on >

Attributes & Claims ...

+ Add new claim
+ Add a group claim
☰ Columns
🗨 Got feedback?

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	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		...
Status	Active	
Thumbprint	FAD4EFA9D35A24CD6E0381159149BDAE59DA4807	
Expiration	2/4/2025, 9:03:50 PM	
Notification Email	u_arsh@hotmail.com	
App Federation Metadata Url	https://login.microsoftonline.com/b5eaf703-f6be ...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

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

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/b5eaf703-f6be ...
Azure AD Identifier	https://sts.windows.net/b5eaf703-f6be-4034-a7d ...
Logout URL	https://login.microsoftonline.com/b5eaf703-f6be ...

[View step-by-step instructions](#)

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**.


Home > Enterprise applications > Home_Orch

Home_Orch | Properties

Enterprise Application

Save Discard Delete Got feedback?

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more](#).

Enabled for users to sign-in?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Name *	Home_Orch
Homepage URL	
Logo	 Select a file
User access URL	https://myapps.microsoft.com/signin/caa1ff00-0cea-4fd1-98a8-972 ...
Application ID	caa1ff00-0cea-4fd1-98a8-9727bbaa21eb
Object ID	44b5268c-97ff-46fe-8a6b-f6fa0e7960ea
Terms of Service Url	Publisher did not provide this information
Privacy Statement Url	Publisher did not provide this information
Reply URL	https://192.168.1.150/gms/rest/authentication/saml2/consume

- **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

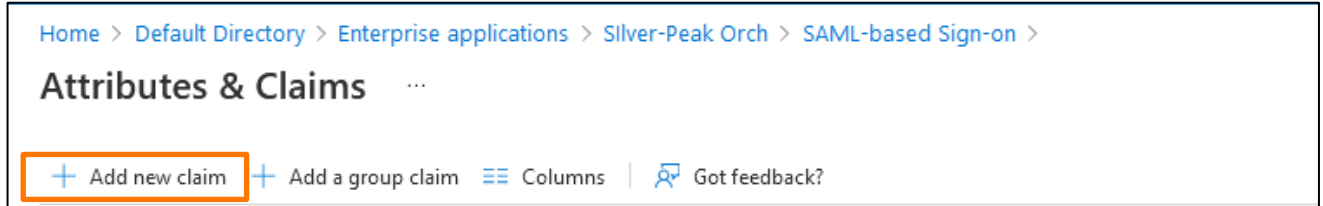
We recommended that you define roles in Azure that map to Orchestrator role-based access control (RBAC). This is helpful for creating different permission levels for different user accounts. The following figure shows the set up for RBAC in Orchestrator that you can map to the Azure AD groups.

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**.

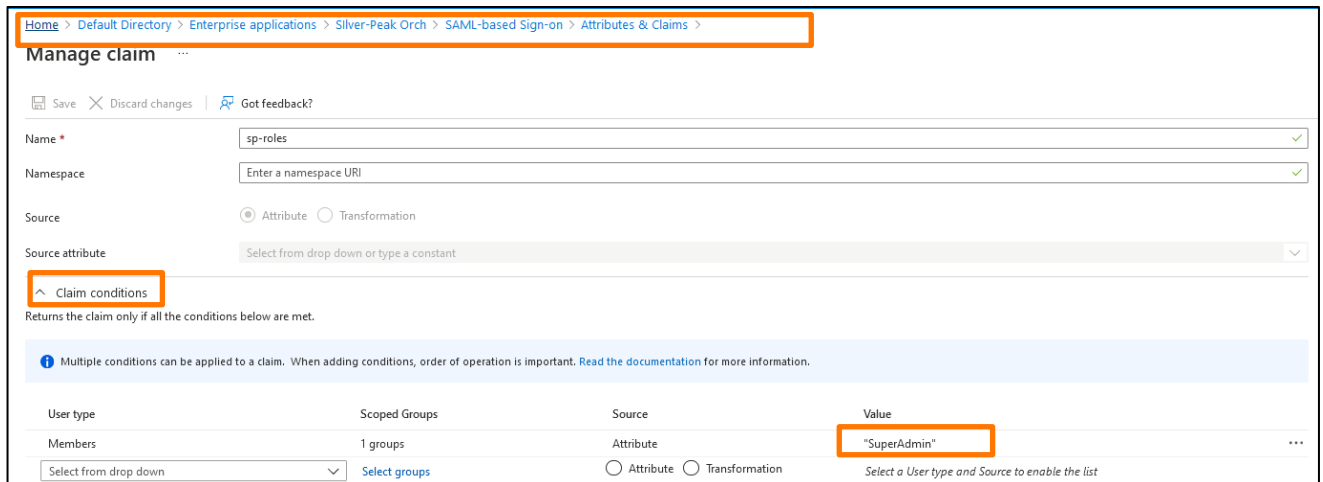
The SAML-based Sign-on page opens.

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

1. Access Orchestrator and go to **Orchestrator > Orchestrator Server > Users & Authentication > Authentication**.
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.”

The screenshot shows a configuration window titled "Remote Authentication Server" with a close button (X) in the top right corner. The window contains several fields for configuring a SAML server:

- Type: SAML (dropdown)
- Name: Umair_Azure_AD
- Username Attribute: http://schemas.xmlsoap.org/ws/20
- Issuer URL: https://sts.windows.net/b5eaf703-f6be-4034-a7d9-d68425e88bac/
- SSO Endpoint: https://myapps.microsoft.com/signin/62397152-65a3-4d8f-8be8-172
- IdP X.509 Cert: -----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQR6HsuucWjqJBsMBILbCfyjANBgkqhkiG
- ACS URL: https://se-wan-east-sewan-orchge-useast1.silverpeak.cloud/gms/... (copy icon)
- SP SLO Endpoint: https://se-wan-east-sewan-orchge-useast1.silverpeak.cloud/gms/... (copy icon)
- IdP SLO Endpoint: (optional)
- SP X.509 Cert SLO: (optional)
- Roles Attribute: sp-roles (optional) - This field is highlighted with an orange border.
- Appliance Access Group Attribute: sp-aag (optional)
- Default role: Select role (dropdown) (optional)

At the bottom right of the window are "Apply" and "Cancel" buttons.

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.

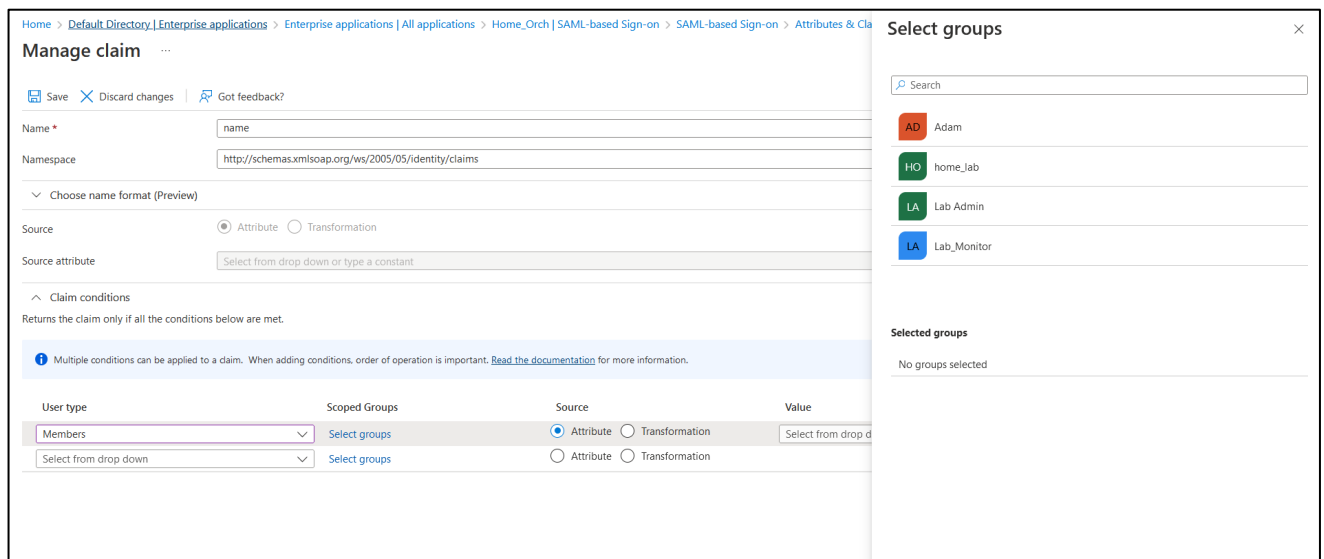
1. In Azure AD, click **Enterprise applications**, then click the name you assigned to Orchestrator, and from the left pane click **Single sign-on**.

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.

User type	Scoped Groups	Source	Value
Members	1 groups	Attribute	"NS_Monitor"
Members	1 groups	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation	"NS_Support_Read"
Members	1 groups	Attribute	"NS_Support_Write"

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.

Members	1 groups	Attribute	"NS_Monitor"	...
Members	1 groups	Attribute	"NS_Monitor, NS_Support"	...
Members	1 groups	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation	"NS_Superadmin"	...

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.