BMS and Azure - SAML 2.0 Single Sign-On (SSO) Just-in-Time (JIT) Provisioning

Release 5.0.0 | Version 1.0

Copyright Agreement

Contents

Azure Setup

IMPORTANT! Please refer to the updated KB here.

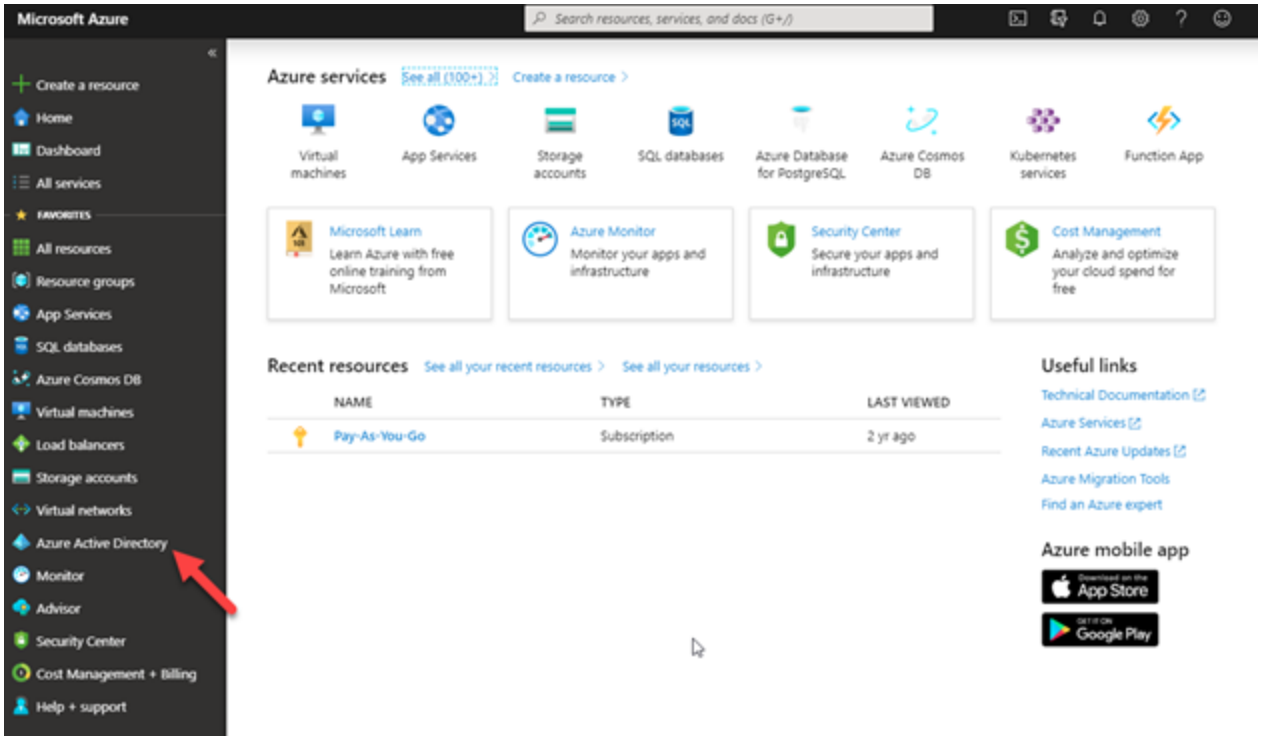
Assuming you have an active Azure (https://portal.azure.com/) account.

In order to setup BMS with Azure you need to add it as a new Enterprise application.

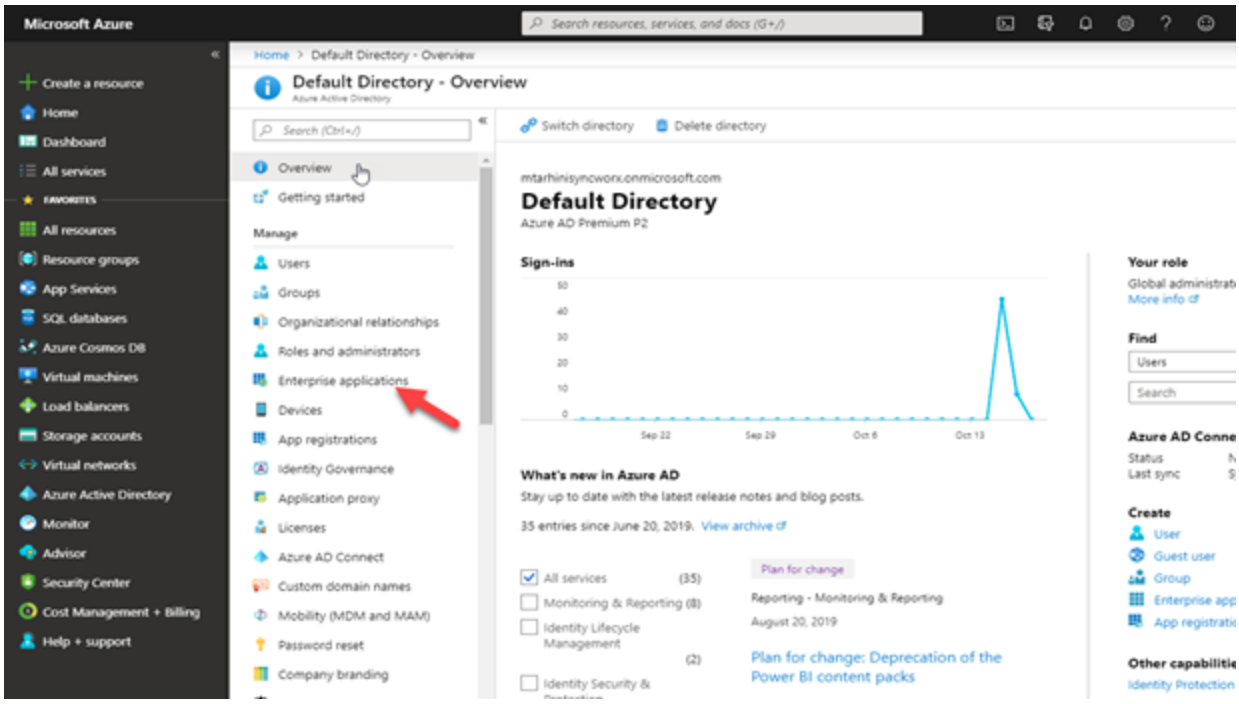
Adding a new application

1 Login to https://portal.azure.com/.

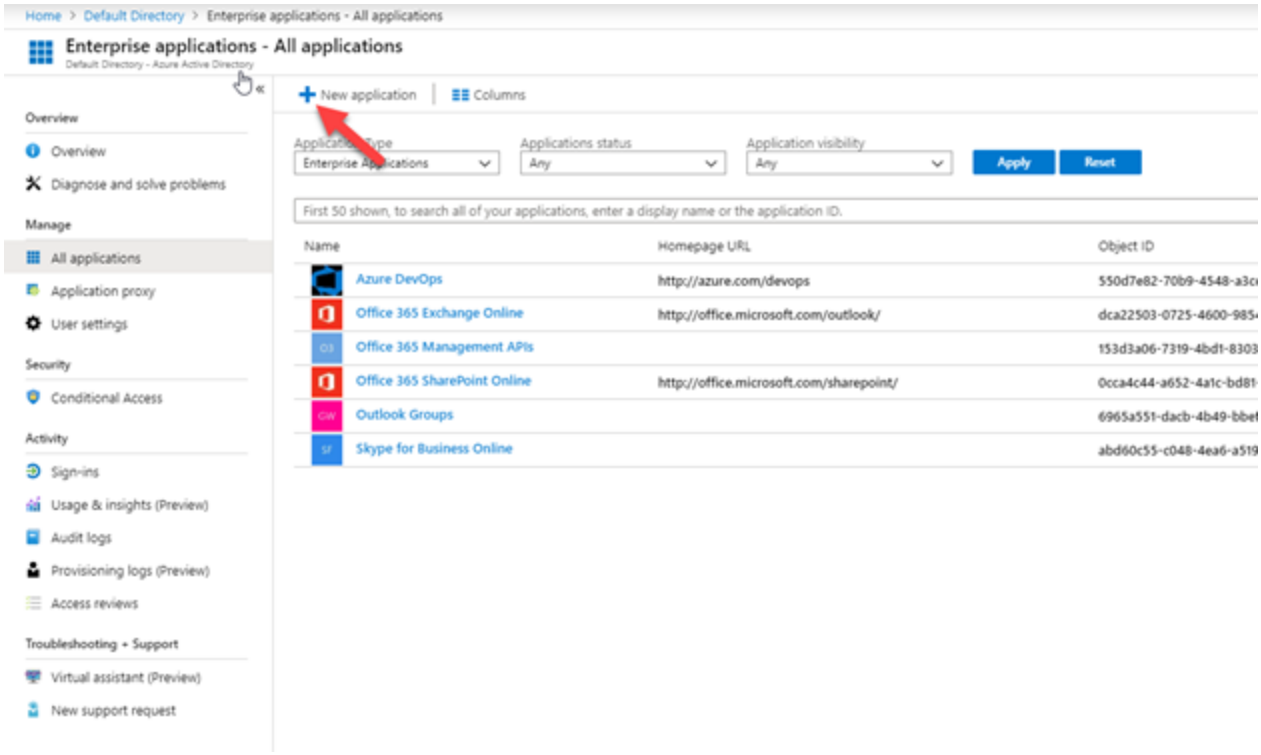
2 In the left-hand menu, select Azure Active Directory.



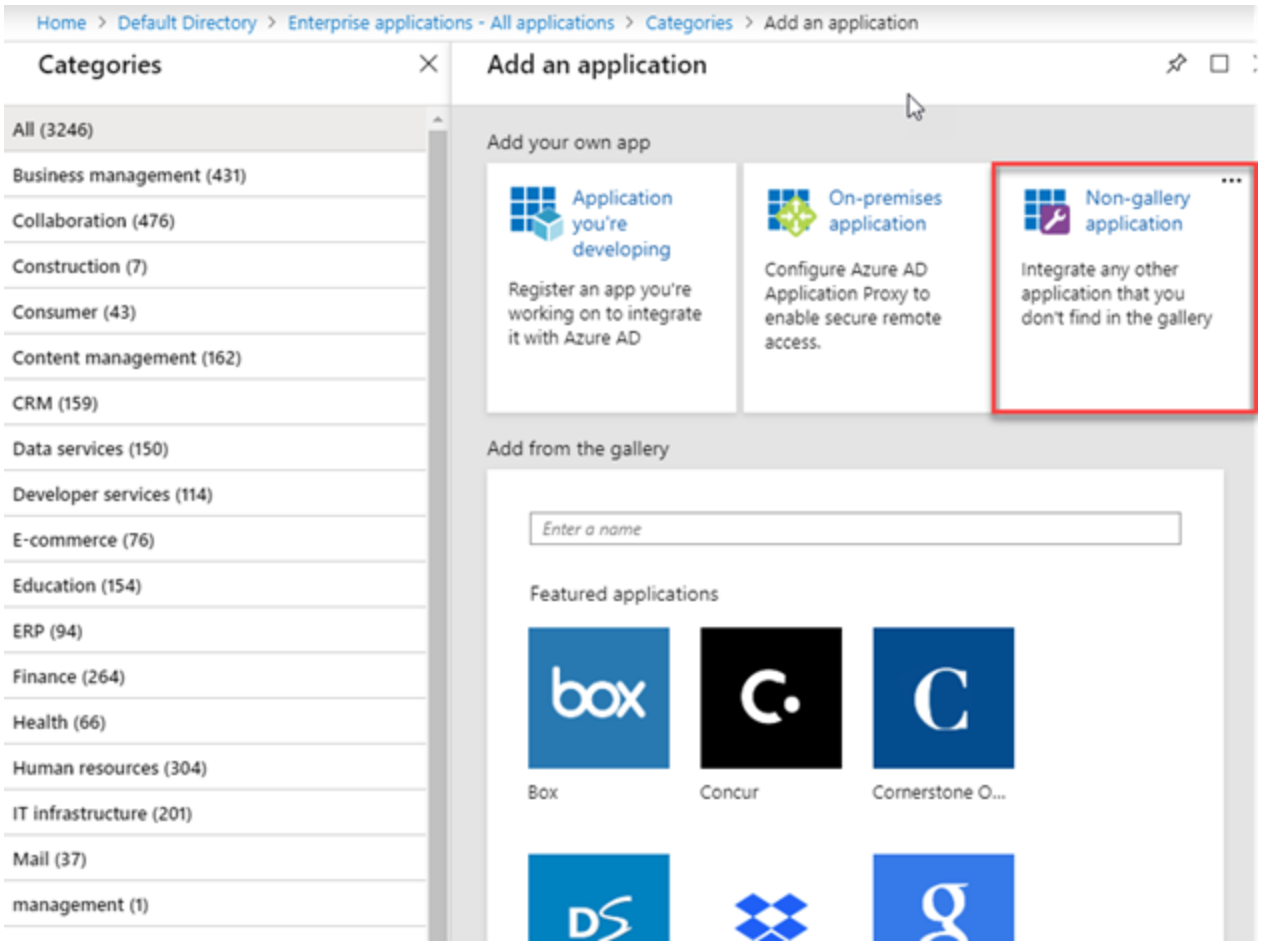
3 Select Enterprise application.



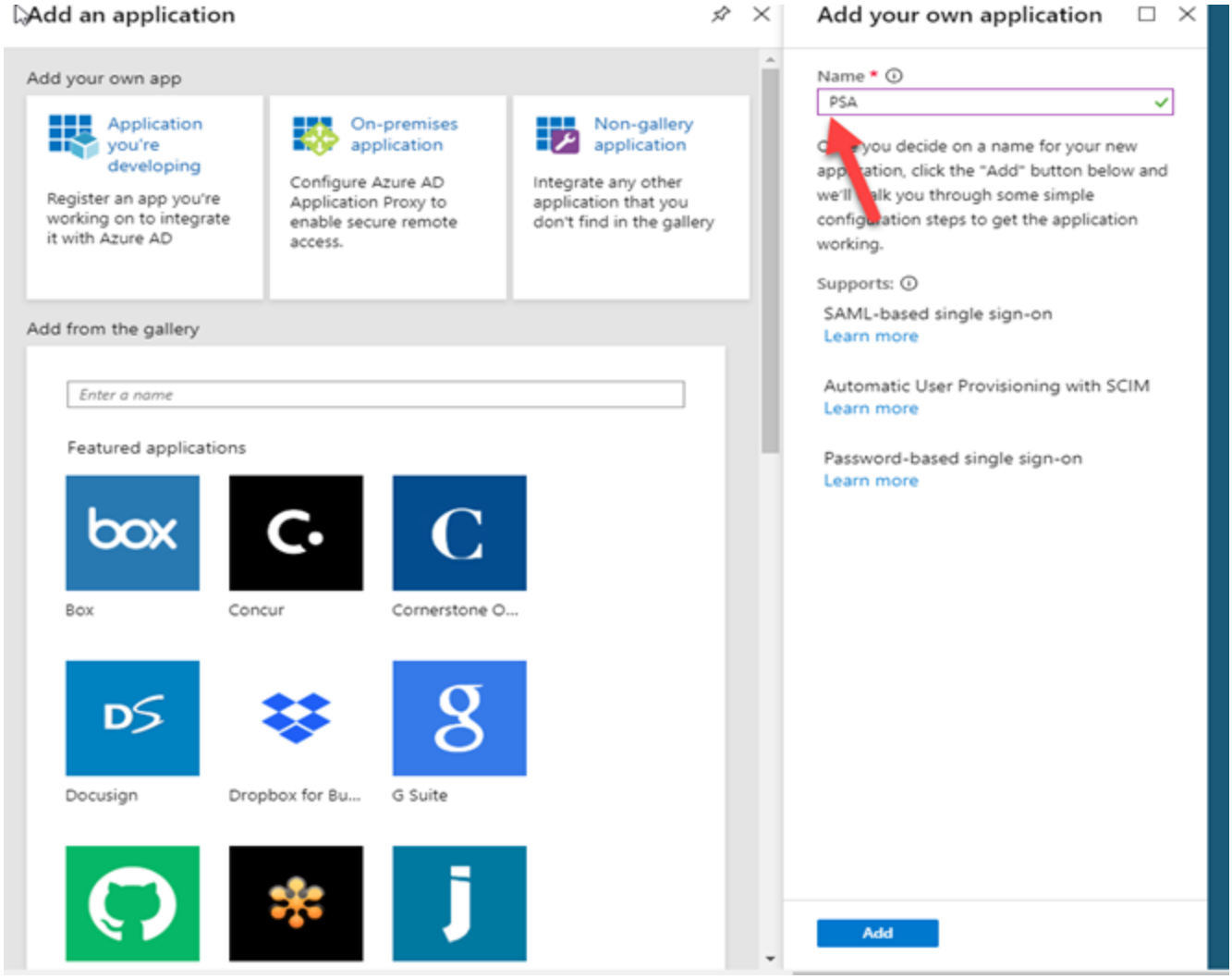
4 Click the **New application**.



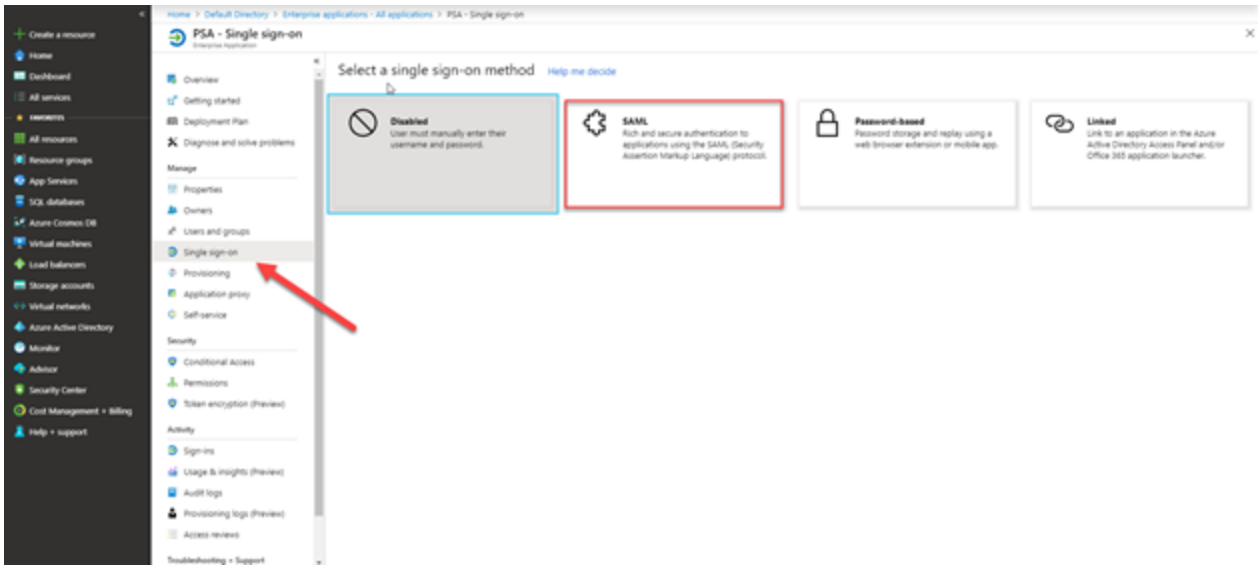
5 Select **Non-gallery application**.



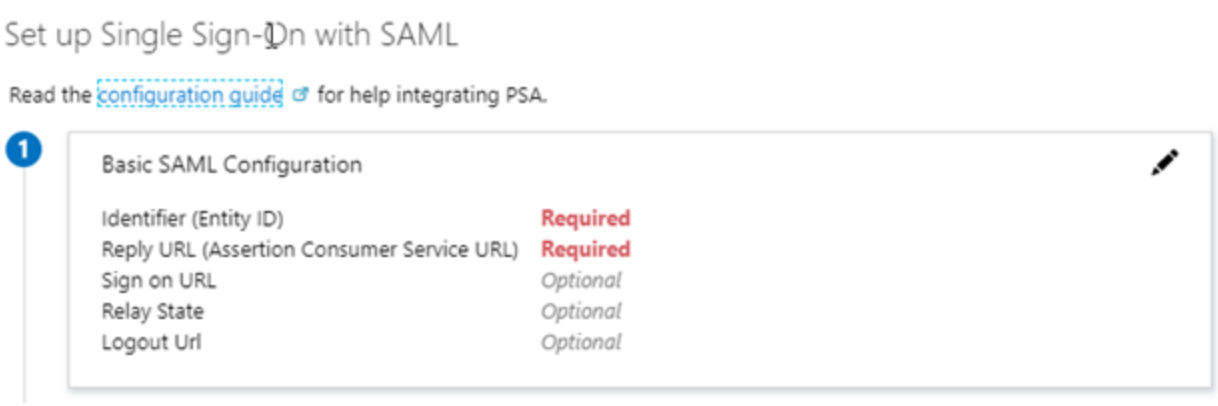
6 Give a name to your new application and then click the **Add** button.



7 Select **Single sign-on** in the menu and then select **SAML**.



8 Edit the **Basic SAML Configuration** box.



9 Enter the following URLs in the fields provided, replacing subdomain with your subdomain:

- Identifier (Entity ID): Enter your BMS domain, e.g. https://bms.kaseya.com
- Reply URL (Assertion Consumer Service URL): Enter https://bms.kaseya.com/SAML/Connect.aspx

10 Return to the setup screen

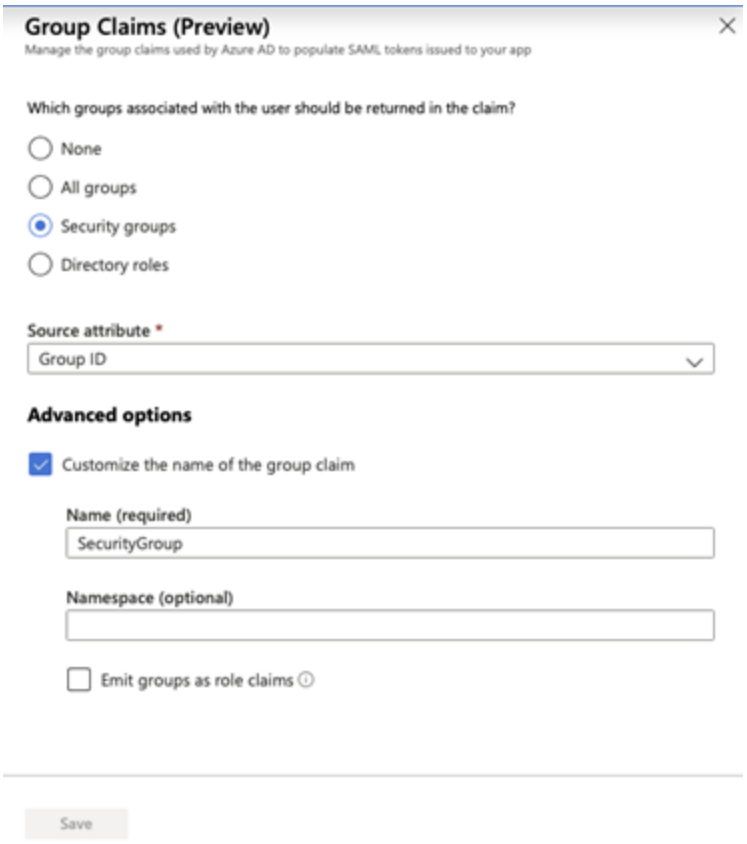
11 Modify the **User Attributes & Claims** box as follows:

- Delete all default Additional claims from the list
- Use the **Add new claim** button to add the following **Claims** (leave **Namespace** blank when adding claims):
  - CompanyName > (enter the **Company Name** as displayed under My Profile in the BMS Web App).
  - Email > user.userprincipalname
  - FirstName > user.givenname
  - LastName > user.surname

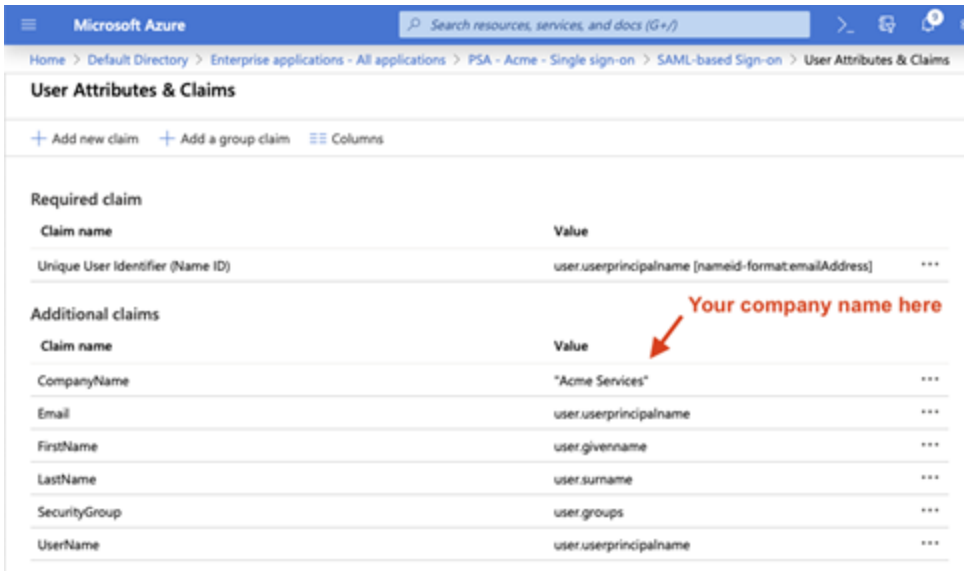
- Username > user.userprincipalname

– Use the Add a group claim button to add a group claim

- Select **Security groups**
- For **Source attribute**, select **Group ID**.
- Under **Advanced Options**, check **Customize the name of the group claim** then enter SecurityGroup as the **Name** and click **Save**.

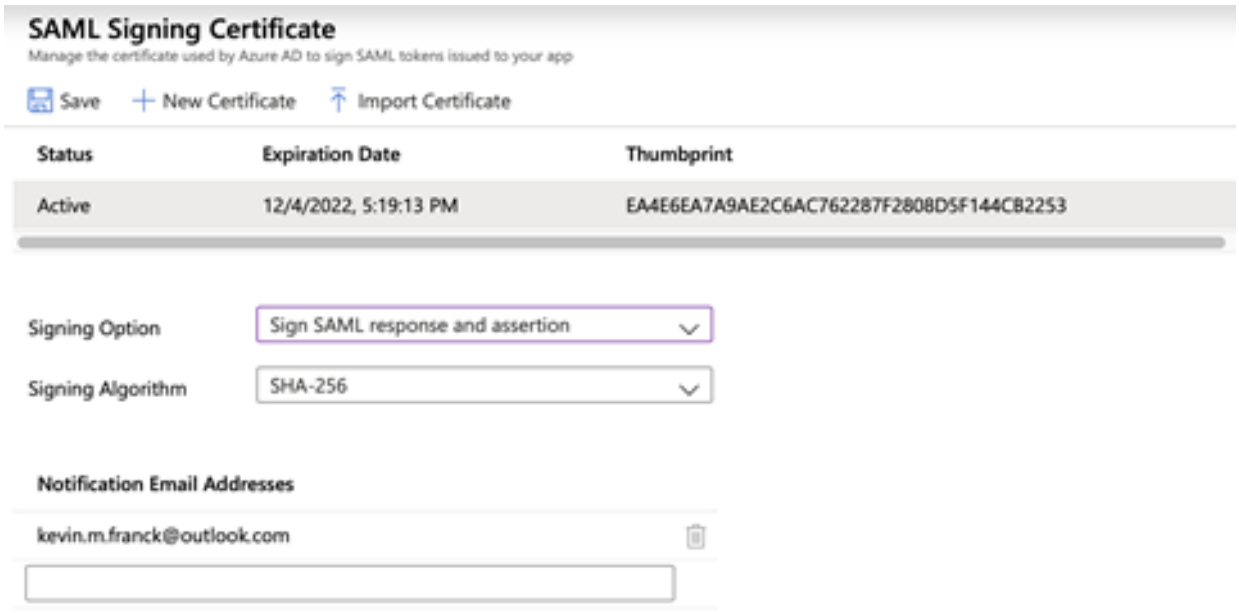


– When complete, the User Attributes & Claims section should look as follows:



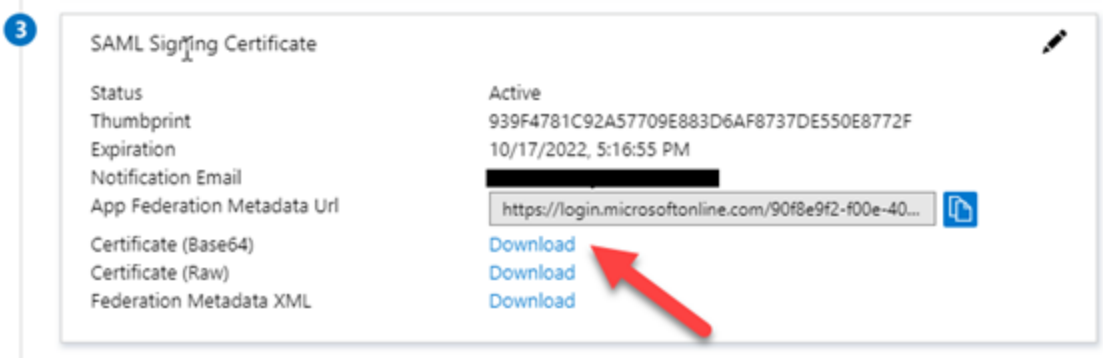
12 Edit the **SAML Signing Certificate** box as follows:

- **Signing Option** – Select **Sign SAML response and assertion**;
- **Signing Algorithm** – Select **SHA-256**;



Download the Certificate

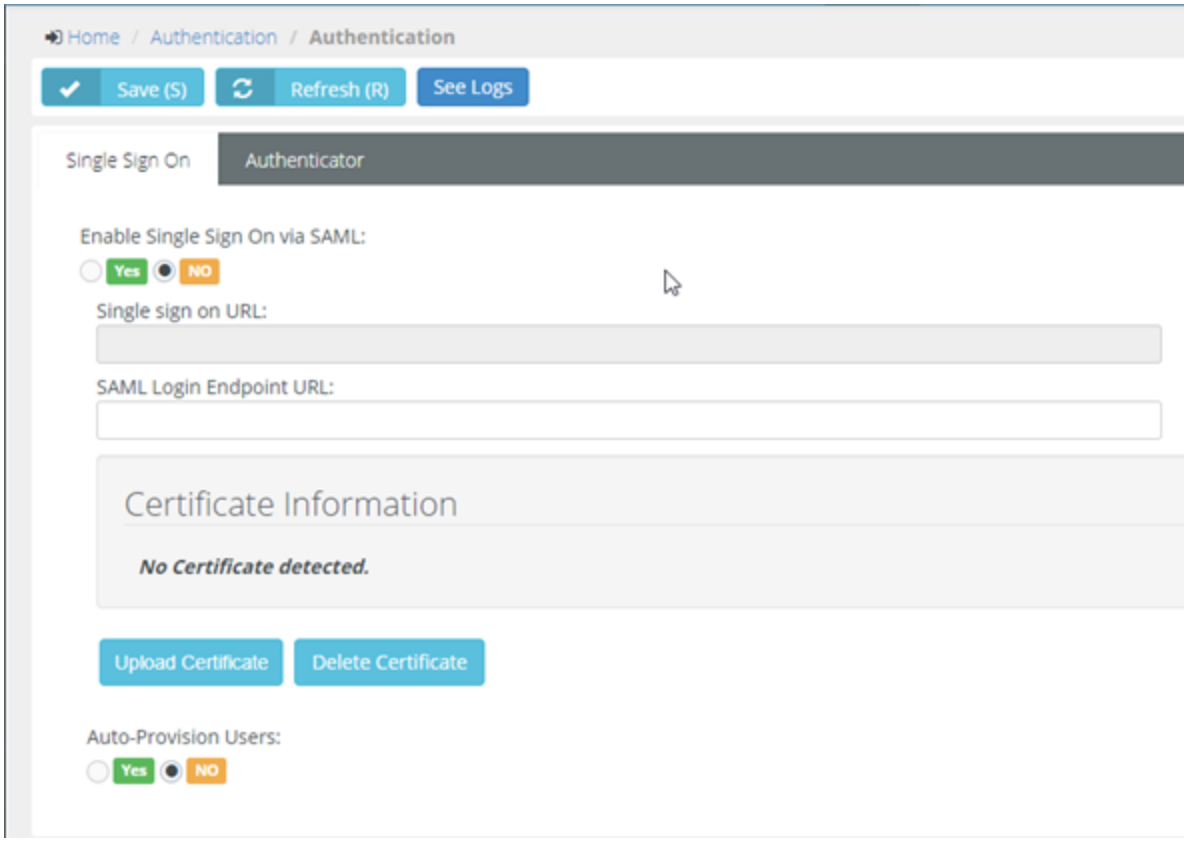
In the setup screen, click **the SAML Signing Certificate** box then download the certificate.



BMS Setup

In BMS you need to setup the system to enable SAML authentication and that can be achieved under **Admin > My Company > Authentication**.

In the "Single Sign On" tab, upload the certificate downloaded previously, and set "Enable Single Sign On via SAML" to **Yes**, then click Save.



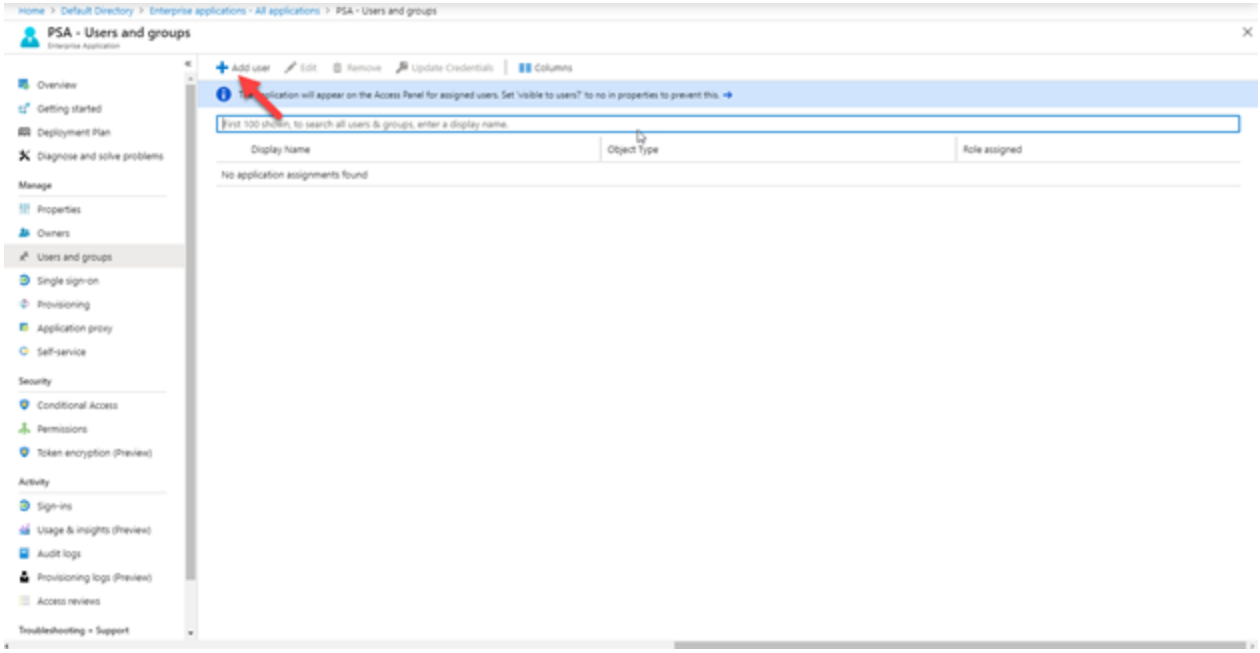
This will enable BMS SAML authentication.

Azure Application Assignment

Once the application created, you have to assign users or user groups to this application.

1 Select the **Users and groups** tab in the left-hand menu.

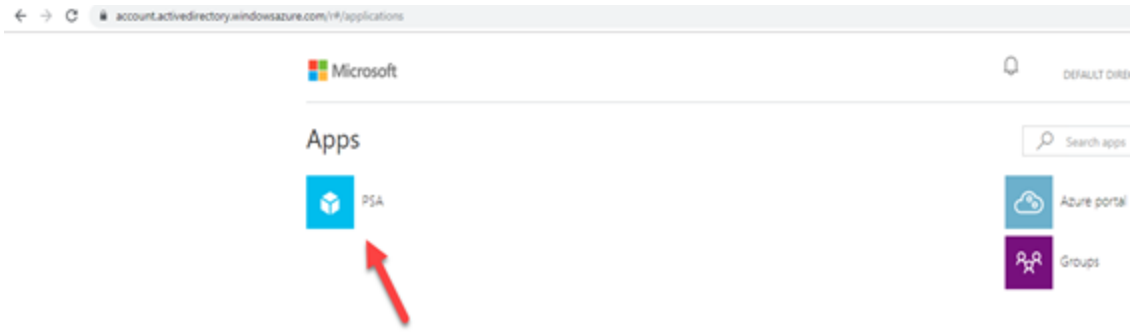
2 Click the **Add user** button to assign users or user groups to this application.



Now when the user assigned, perform the following steps to make sure that SSO is working:

1 Log out and close the Azure management portal and the Azure AD access panel.

2 In a new browser session, navigate directly to the access panel at http://myapps.microsoft.com.

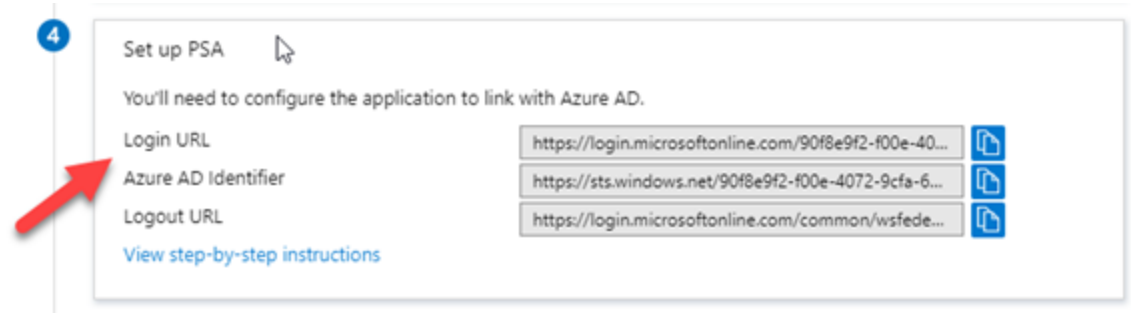


3 Enter your Azure AD credentials to log in. After authentication, you will be able to interact with the applications integrated with the directory.

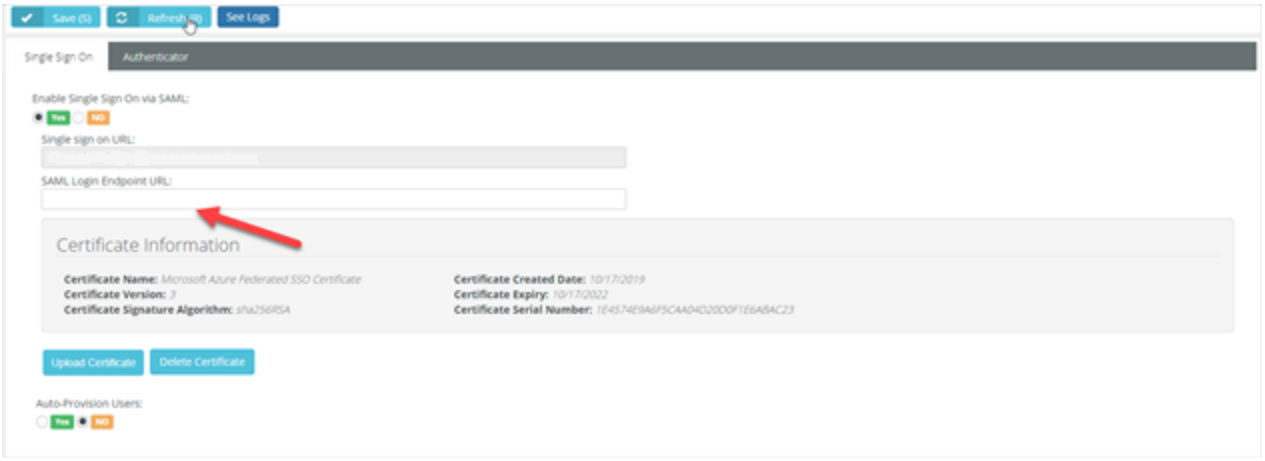
4 Click on the BMS SSO application you created to be redirected and logged in to BMS.

Enable Two Way SAML Login

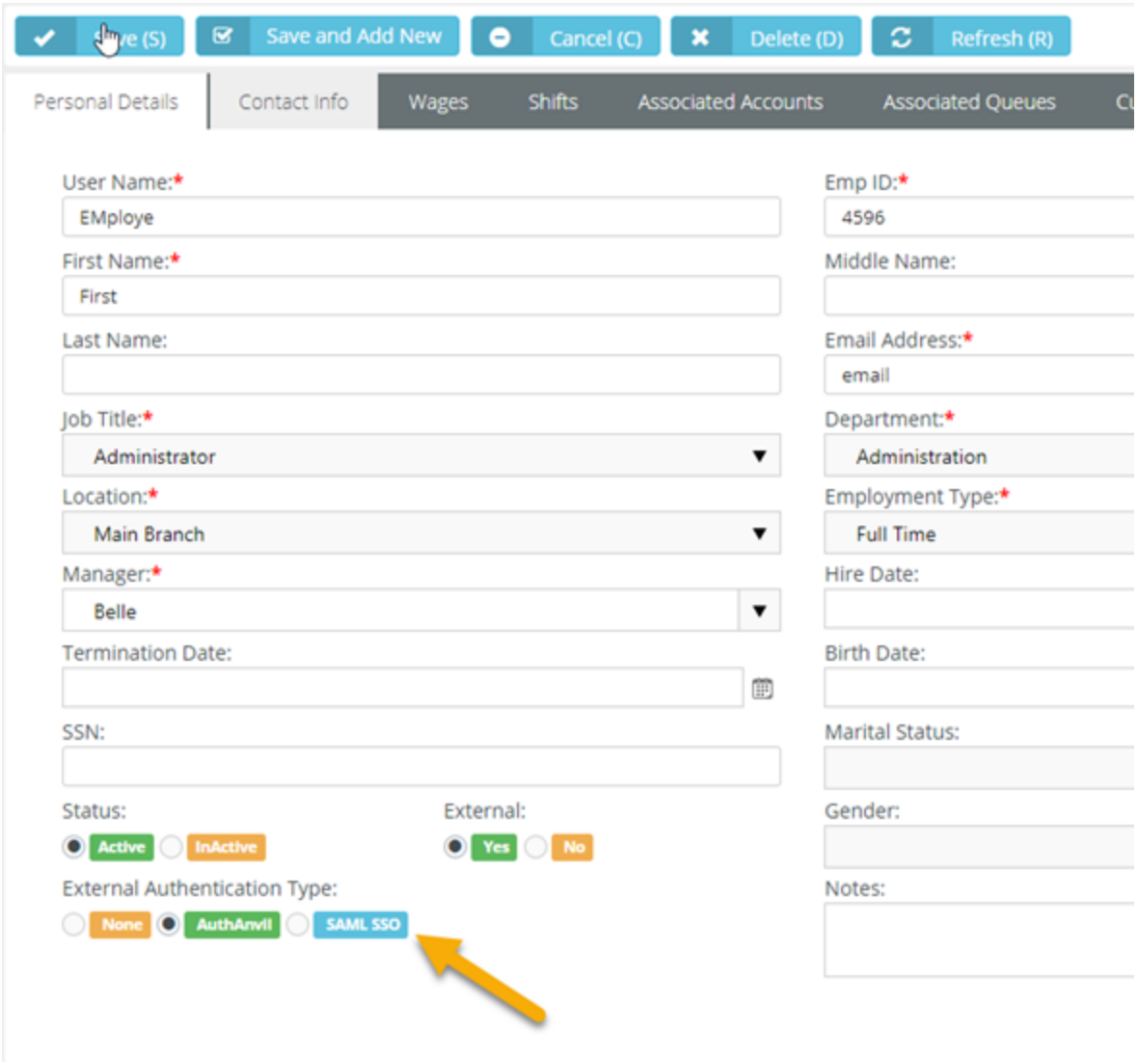
In order to launch Azure during the Log in from BMS. You need to enable two-way SAML integration. In order to do this, you will need your Azure Login URL that can be found here:



Once you have this URL, you will need to save it in BMS under the Authentication Page:

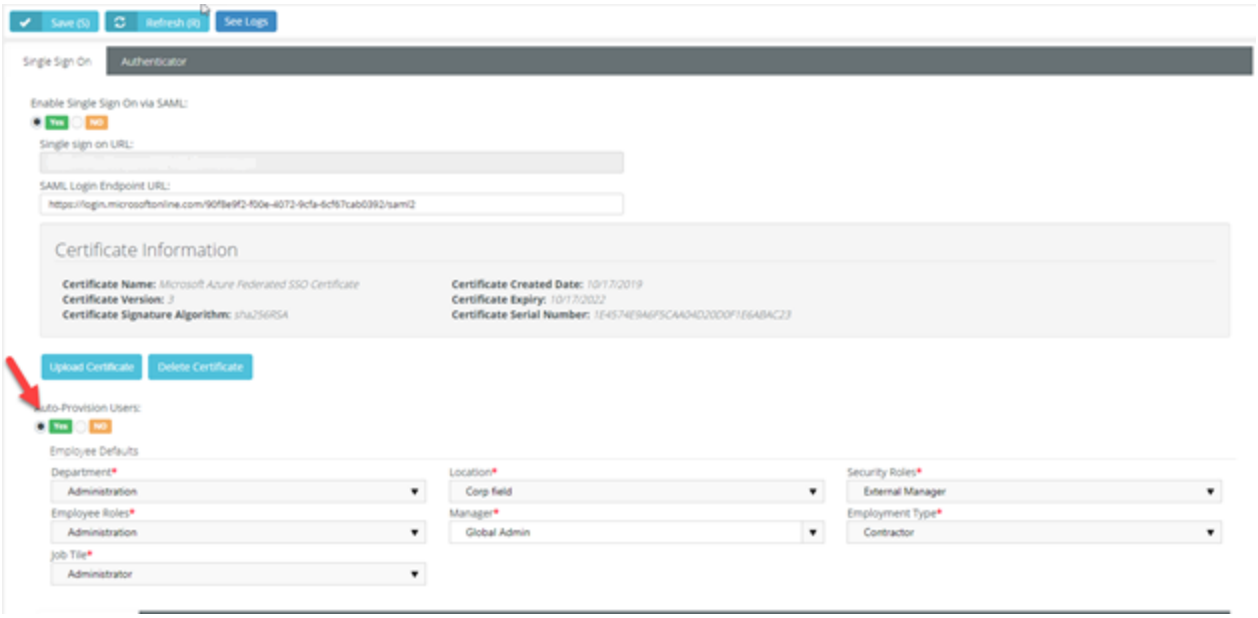


This will allow you to leverage the Azure Log in screen when users are trying to log in to BMS. You can enable this on the User Level by updating the Authentication Type on the Employee Level:

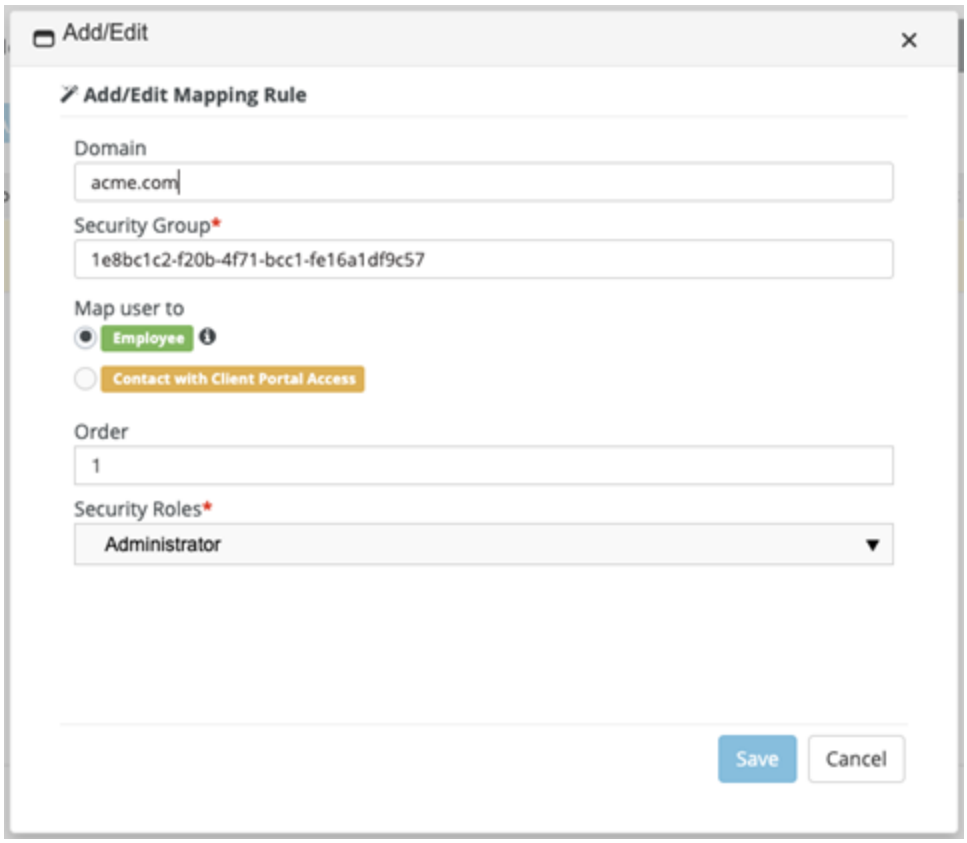

Save and Add New
Cancel (C)
Delete (D)
Refresh (R)
Personal Details
Contact Info
Wages
Shifts
Associated Accounts
Associated Queues
User Name:*
EMployee
Emp ID:*
4596
First Name:*
First
Middle Name:
Last Name:
Email Address:*
email
Job Title:*
Administrator
Department:*
Administration
Location:*
Main Branch
Employment Type:*
Full Time
Manager:*
Belle
Hire Date:
Termination Date:
Birth Date:
SSN:
Marital Status:
Status:
Active
InActive
External:
Yes
No
Gender:
External Authentication Type:
None
AuthAnvil
SAML SSO
Notes:

Enable JIT Provisioning

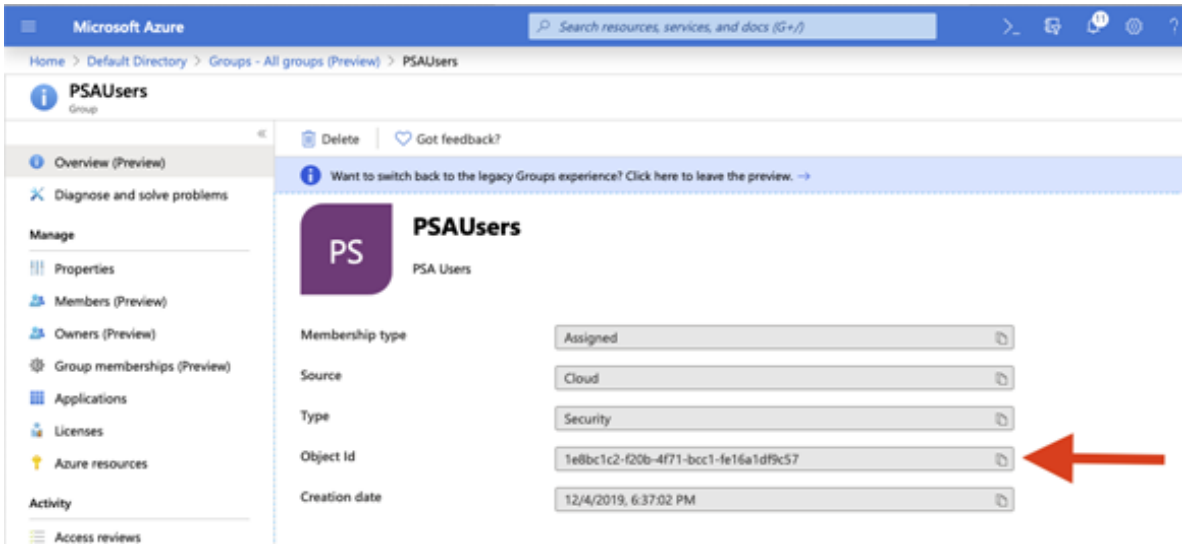
In order to enable Just-in-Time (JIT) provisioning, you will need to do it from the BMS Authentication page.



By default, all Users will take the Default Security Roles specified in the above Employee Defaults Section. In order to start mapping Active Directory Groups to BMS Security Roles you will need to Add Mapping Rules as following:



Note: For Security Group, you must use the 'Object Id' value associated with the Group in Azure AD.



By adding multiple Rules, you can now start routing Active Directory Users to BMS Security Roles based on Domain and Security Group.