

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

Release 5.0.0 | Version 1.0



Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at <http://www.kaseya.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement.

Contents

Azure Setup	4
Download the Certificate	11
BMS Setup	12
Azure Application Assignment	13
Enable Two Way SAML Login	14
Enable JIT Provisioning	16

Azure Setup

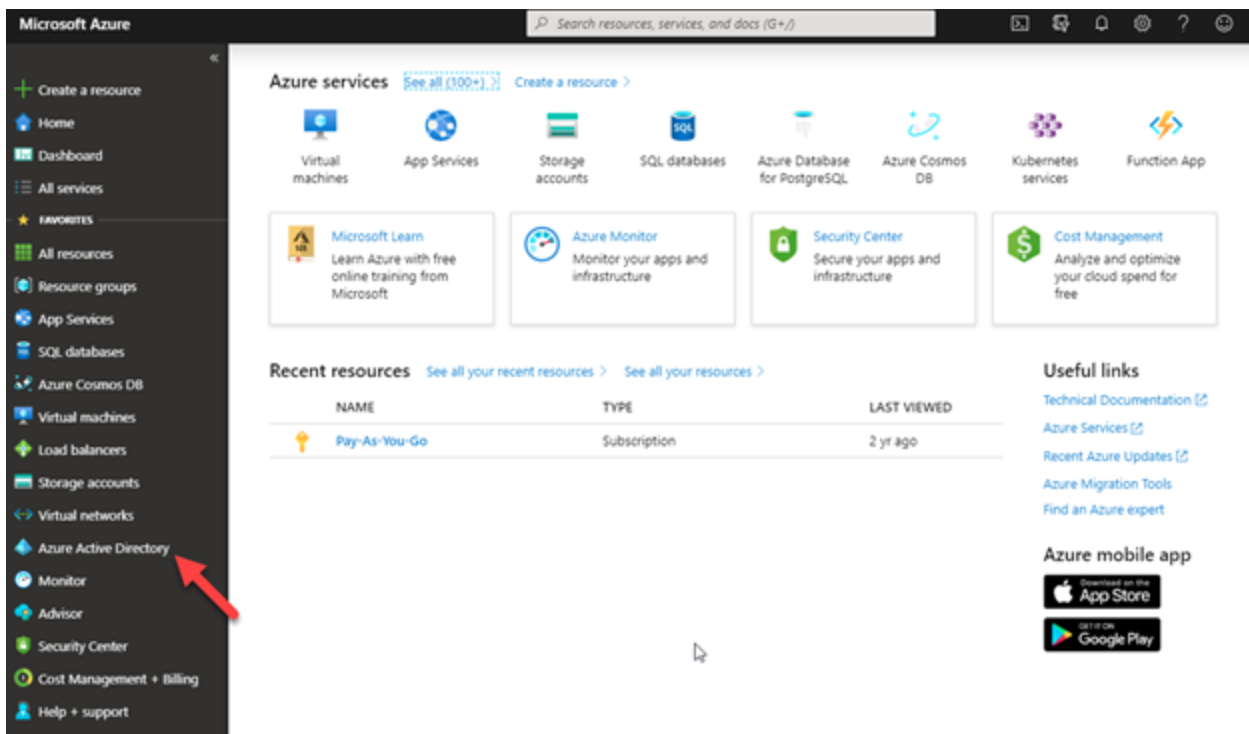
IMPORTANT! Please refer to the updated KB [here](#).

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

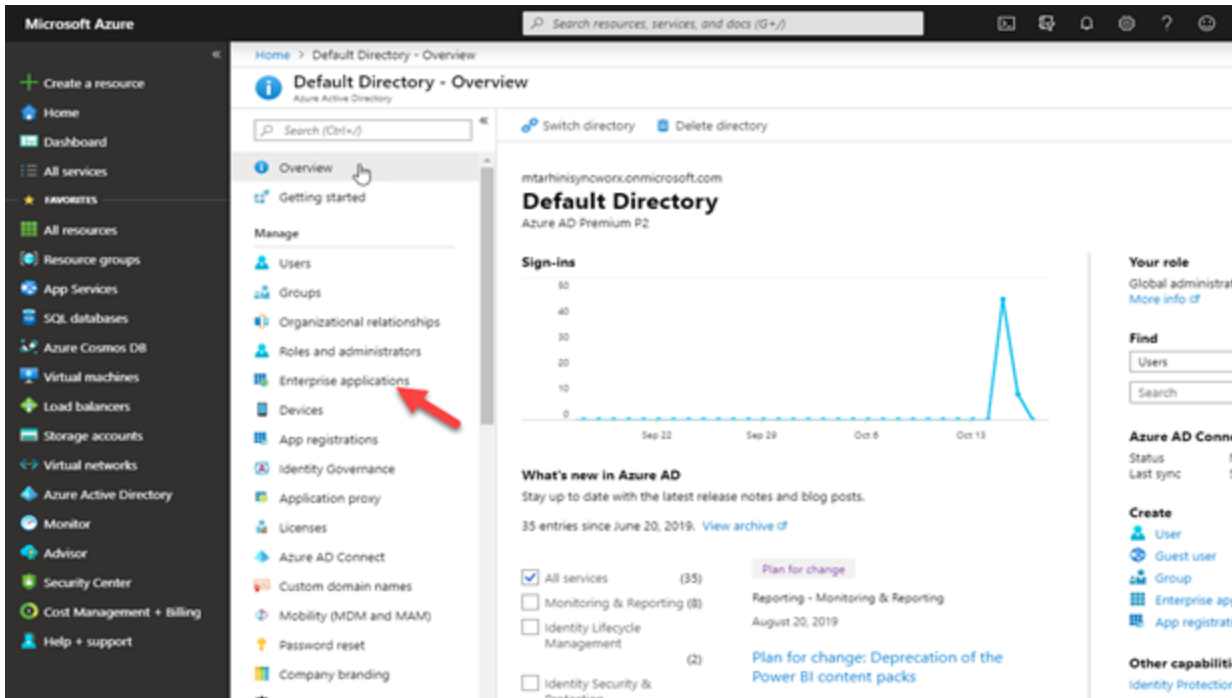
In order to setup BMS with Azure you need to add it as a new Enterprise application.

Adding a new application

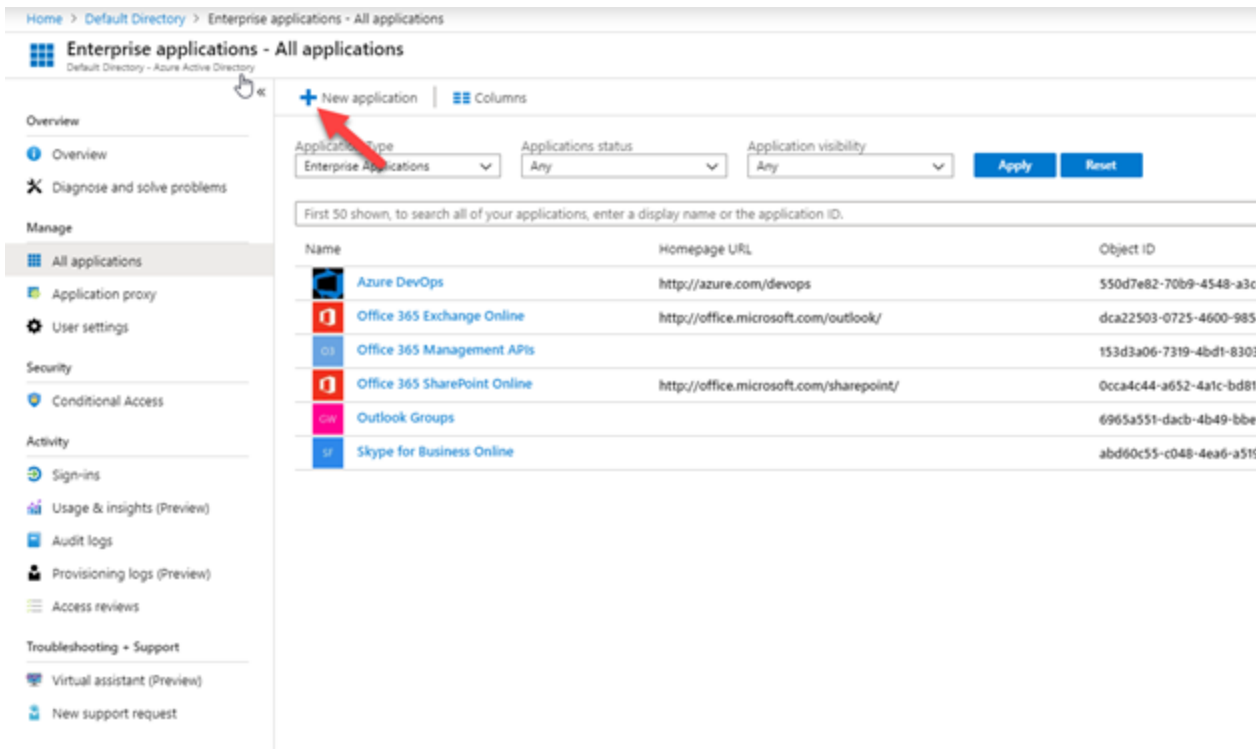
- 1 Login to <https://portal.azure.com/>.
- 2 In the left-hand menu, select Azure Active Directory.



- 3 Select Enterprise application.



4 Click the New application.



5 Select Non-gallery application.

Home > Default Directory > Enterprise applications - All applications > Categories > Add an application

Categories

- All (3246)
- Business management (431)
- Collaboration (476)
- Construction (7)
- Consumer (43)
- Content management (162)
- CRM (159)
- Data services (150)
- Developer services (114)
- E-commerce (76)
- Education (154)
- ERP (94)
- Finance (264)
- Health (66)
- Human resources (304)
- IT infrastructure (201)
- Mail (37)
- management (1)

Add an application

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**
Integrate any other application that you don't find in the gallery

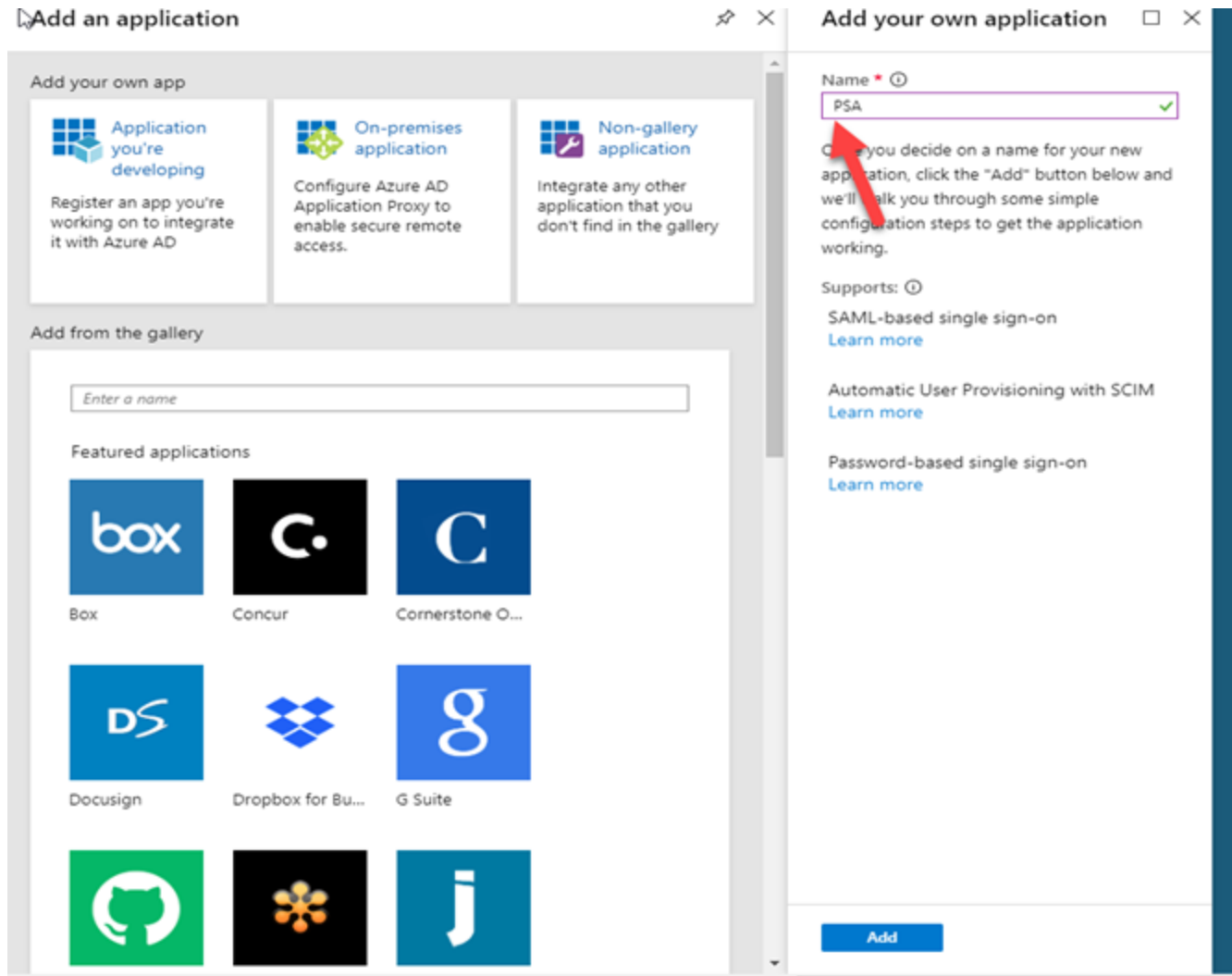
Add from the gallery

Enter a name

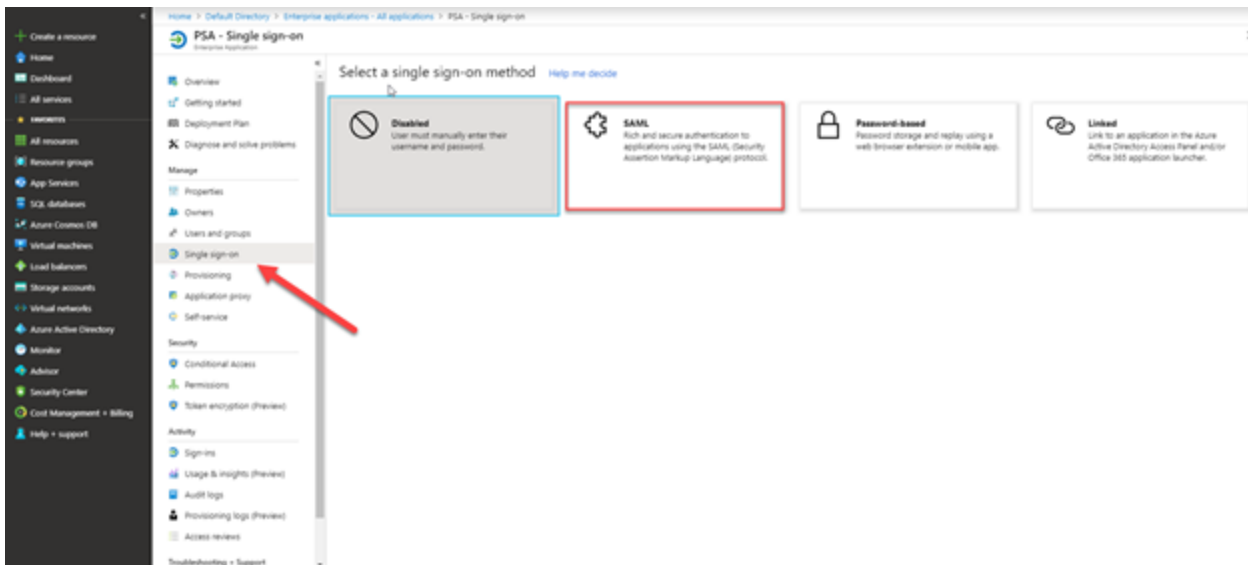
Featured applications

- Box
- Concur
- Cornerstone O...
- DS
-
- g

- 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.

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating PSA.

1 Basic SAML Configuration ✎

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

- 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**.

Group Claims (Preview) X

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None

All groups

Security groups

Directory roles

Source attribute *

Group ID

Advanced options

Customize the name of the group claim

Name (required)

SecurityGroup

Namespace (optional)

Emit groups as role claims ⓘ

Save

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

Microsoft Azure

Home > Default Directory > Enterprise applications > All applications > PSA - Acme - Single sign-on > SAML-based Sign-on > User Attributes & Claims

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress] ***

Additional claims

Claim name	Value
CompanyName	"Acme Services" ***
Email	user.userprincipalname ***
FirstName	user.givenname ***
LastName	user.surname ***
SecurityGroup	user.groups ***
UserName	user.userprincipalname ***

Your company name here

12 Edit the SAML Signing Certificate box as follows:

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

SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save + New Certificate Import Certificate

Status	Expiration Date	Thumbprint
Active	12/4/2022, 5:19:13 PM	EA4E6EA7A9AE2C6AC762287F2808D5F144CB2253

Signing Option: Sign SAML response and assertion

Signing Algorithm: SHA-256

Notification Email Addresses

kevin.m.franck@outlook.com


Download the Certificate

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

3

SAML Signing Certificate

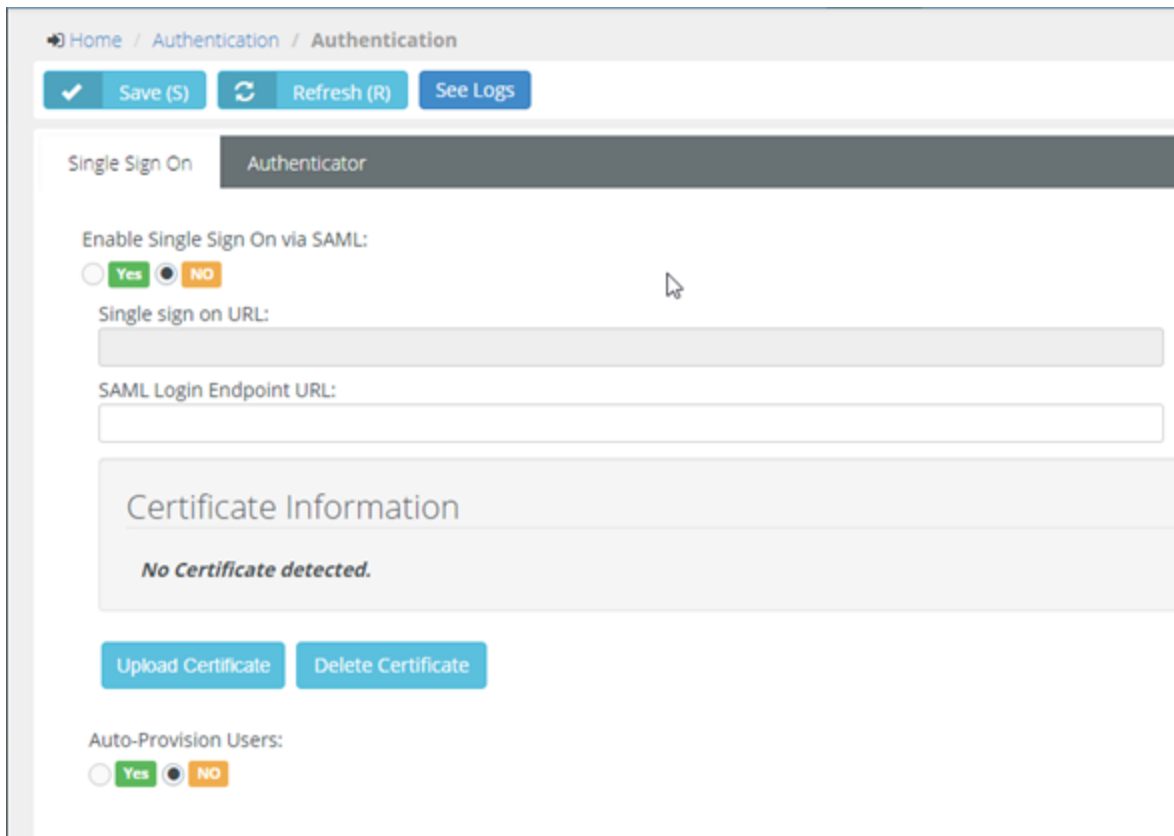
Status	Active
Thumbprint	939F4781C92A57709E883D6AF8737DE550E8772F
Expiration	10/17/2022, 5:16:55 PM
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/90f8e9f2-f00e-40...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download



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.



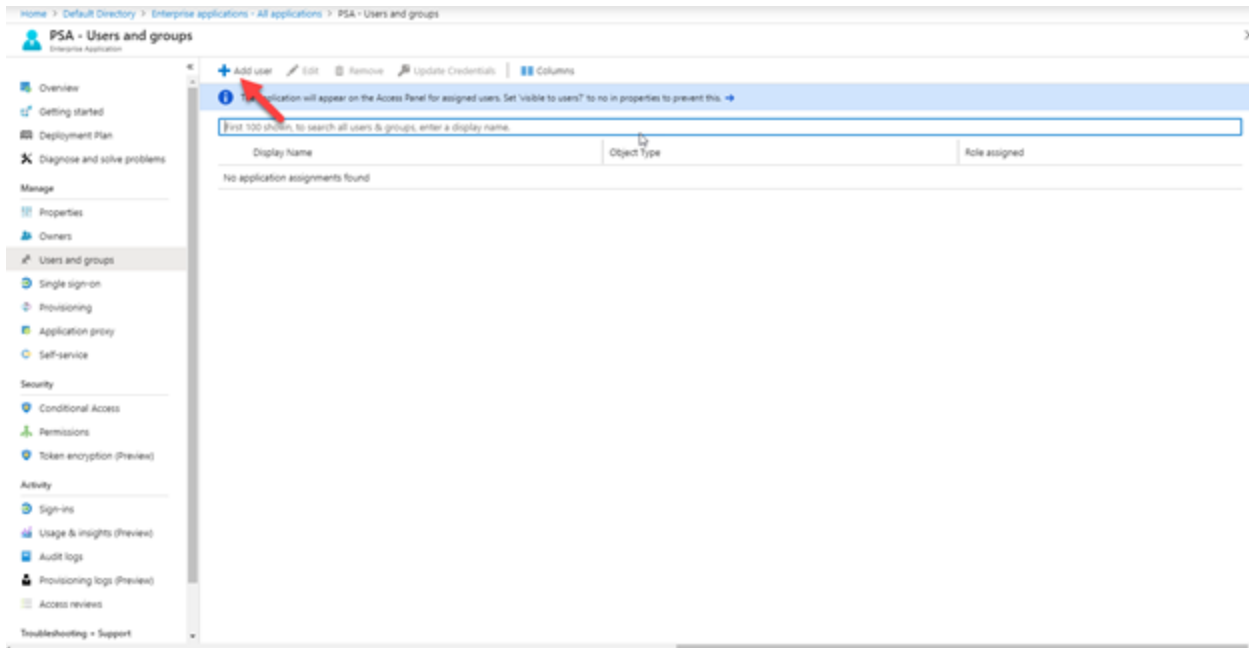
The screenshot shows the BMS Authentication configuration page. The breadcrumb navigation is Home / Authentication / Authentication. There are three buttons at the top: Save (S), Refresh (R), and See Logs. The page has two tabs: Single Sign On and Authenticator. Under the Single Sign On tab, there is a section for "Enable Single Sign On via SAML:" with radio buttons for Yes and NO. The NO option is selected. Below this are two input fields: "Single sign on URL:" and "SAML Login Endpoint URL:". A section titled "Certificate Information" displays the message "No Certificate detected." Below this are two buttons: "Upload Certificate" and "Delete Certificate". At the bottom, there is a section for "Auto-Provision Users:" with radio buttons for Yes and NO. The NO option is selected.

This will enable BMS SAML authentication.

Azure Application Assignment

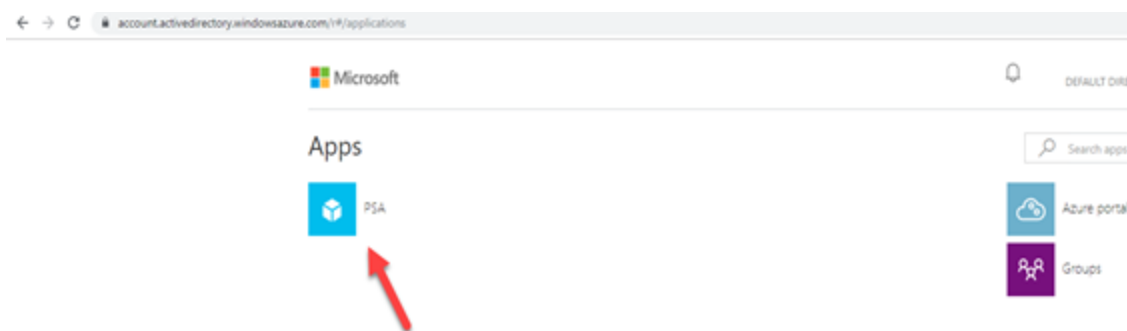
Once the application created, you have to assign users or user groups to this application.

- 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:

4 Set up PSA

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

Login URL: `https://login.microsoftonline.com/90f8e9f2-f00e-40...`

Azure AD Identifier: `https://sts.windows.net/90f8e9f2-f00e-4072-9cfa-6...`

Logout URL: `https://login.microsoftonline.com/common/wsfede...`

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

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

Save (S) Refresh (R) See Logs

Single Sign On: Authenticator

Enable Single Sign On via SAML: Yes No

Single sign on URL:

SAML Login Endpoint URL:

Certificate Information

Certificate Name: Microsoft Azure Federated SSO Certificate	Certificate Created Date: 10/17/2019
Certificate Version: 3	Certificate Expiry: 10/17/2022
Certificate Signature Algorithm: sha256RSA	Certificate Serial Number: 1E4574E9B6F5CA4D20D0F1E6BAC23

Upload Certificate Delete Certificate

Auto-Provision Users: Yes No

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 (S) Save and Add New Cancel (C) Delete (D) Refresh (R)

Personal Details | Contact Info | **Wages** | Shifts | Associated Accounts | Associated Queues | C

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

External Authentication Type:
 None AuthArvill SAML SSO

Gender:

Notes:



Enable JIT Provisioning

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

The screenshot shows the BMS Authentication page with the following configuration:

- Single Sign On:** Autheticator
- Enable Single Sign On via SAML:** Yes No
- Single sign on URL:** [Empty text box]
- SAML Login Endpoint URL:** `https://login.microsoftonline.com/9073e9f2-450e-4072-9cfa-6c97cab0392/saml2`
- Certificate Information:**
 - Certificate Name:** Microsoft Azure Federated SSO Certificate
 - Certificate Version:** 3
 - Certificate Signature Algorithm:** sha256RSA
 - Certificate Created Date:** 10/17/2019
 - Certificate Expiry:** 10/17/2022
 - Certificate Serial Number:** 1E4574E8A6F5CAA0D200F1E6A8AC23
- Buttons:** Upload Certificate, Delete Certificate
- Auto-Provision Users:** Yes No
- Employee Defaults:**
 - Department:** Administration
 - Location:** Corp field
 - Security Roles:** External Manager
 - Employee Roles:** Administration
 - Manager:** Global Admin
 - Employment Type:** Contractor
 - Job Title:** Administrator

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:

Add/Edit Mapping Rule

Domain: acme.com

Security Group*: 1e8bc1c2-f20b-4f71-bcc1-fe16a1df9c57

Map user to: Employee Contact with Client Portal Access

Order: 1

Security Roles*: Administrator

Save Cancel

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

Microsoft Azure

Home > Default Directory > Groups - All groups (Preview) > PSAUsers

PSAUsers
Group

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: 1e8bc1c2-f20b-4f71-bcc1-fe16a1df9c57

Creation date: 12/4/2019, 6:37:02 PM

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