



Integration with Azure SAML

Date: 01/03/2023



How SAML protocol works?

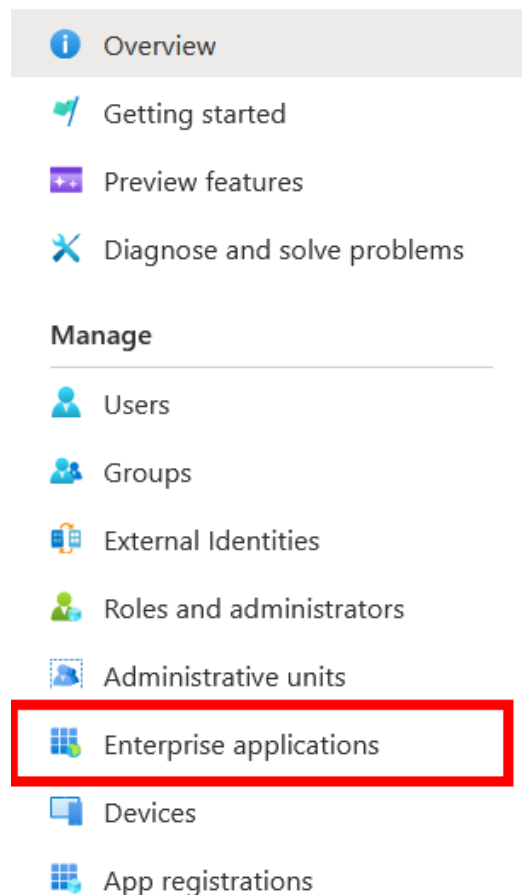
The SAML protocol allows you to log in to the Essentials MDM administrator console via external services (Identity Provider).

The user can login to IdP and choose Essentials MDM among the applications and will be automatically logged into Essentials MDM with IdP credentials. If the user does not have an account in Essentials MDM, such an account can be created automatically (provided that *Automatically create users* is selected in the Essentials MDM settings). After logging out of Essentials MDM, the user can log in again using the **Log in using SAML** button, which will direct you to the login page in IdP. One of such IdP is Microsoft Azure.

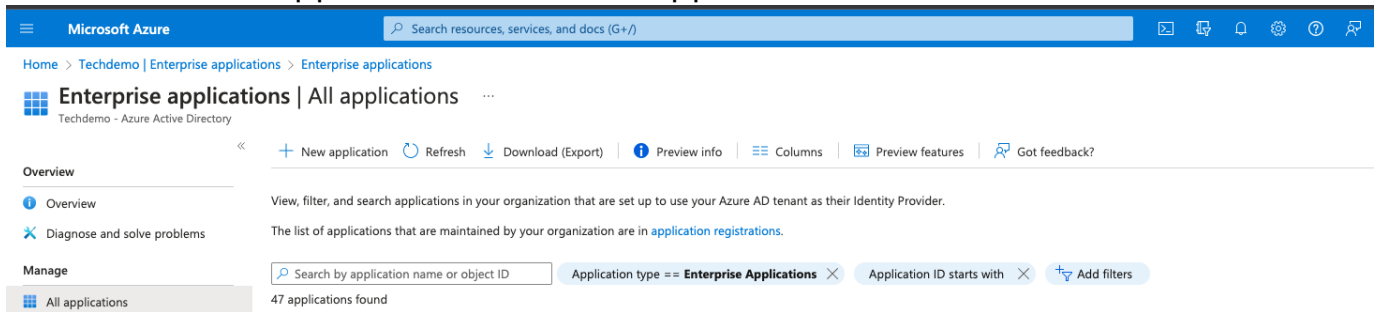
Adding new application in Azure portal

To integrate Essentials MDM with Azure SAML, you will need to create a Essentials MDM application in Azure and then configure data from Azure.

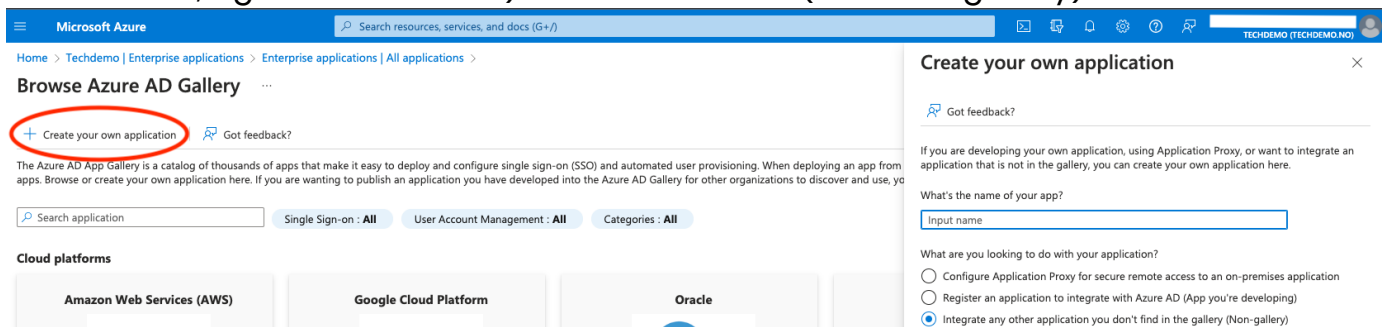
1. Login to the Microsoft Azure portal through the URL <https://portal.azure.com>.
2. Select Azure Active Directory. Then select the Enterprise Applications option from the panel on the left.



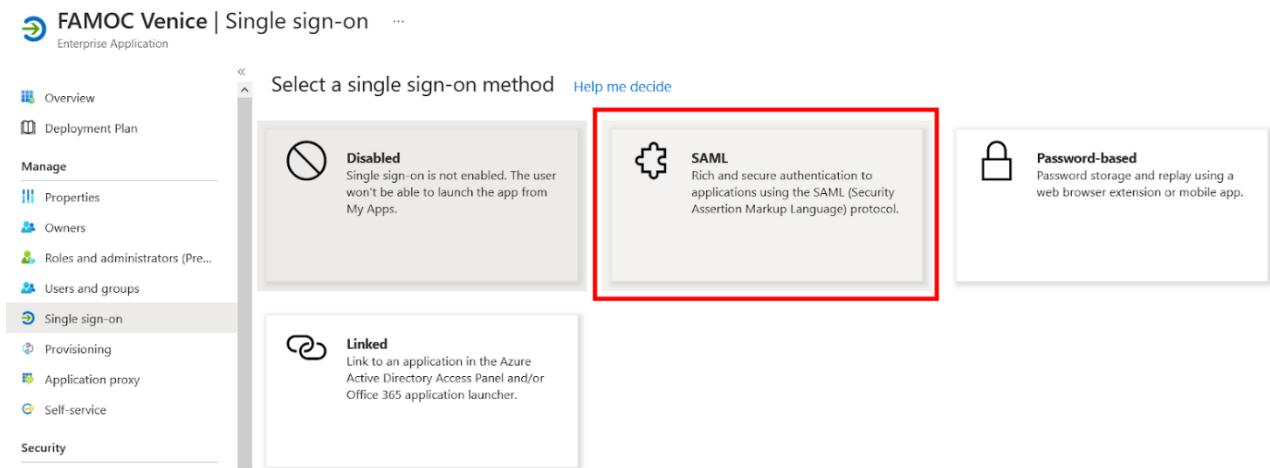
3. To add an application, click +New application.



4. Select Create your own application, enter the name of the application (any name, eg Essentials MDM) and click create. (Use Non-gallery)



5. Go to Manage - Single Sign-On -> SAML



6. Complete the following fields:

Identifier (Entity ID) – it can be your Essentials MDM server URL or any other value, e.g. essentials.yourorganization.com (the same value will need to be provided as EntityId parameter in Essentials SAML settings); Note, mark this value as *Default*.

Reply URL (Assertion Consumer Service URL): <https://serveraddress.com/ui/> (necessarily with / ui / at the end).

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
<input type="text" value="https://venice.fancyfon.com/ui/"/>	<input checked="" type="checkbox"/> ⓘ
<input type="text"/>	

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
<input type="text" value="https://venice.fancyfon.com/ui/"/>	<input checked="" type="checkbox"/> ⓘ
<input type="text"/>	

Save changes and close this section.

7. In the User Attributes & Claims section, leave only the Unique User Identifier – the rest of these identifiers can be removed. This one must remain, in addition, in editing this identifier, you must set “Windows domain qualified name” in “Choose name identifier format”.

Save Discard changes

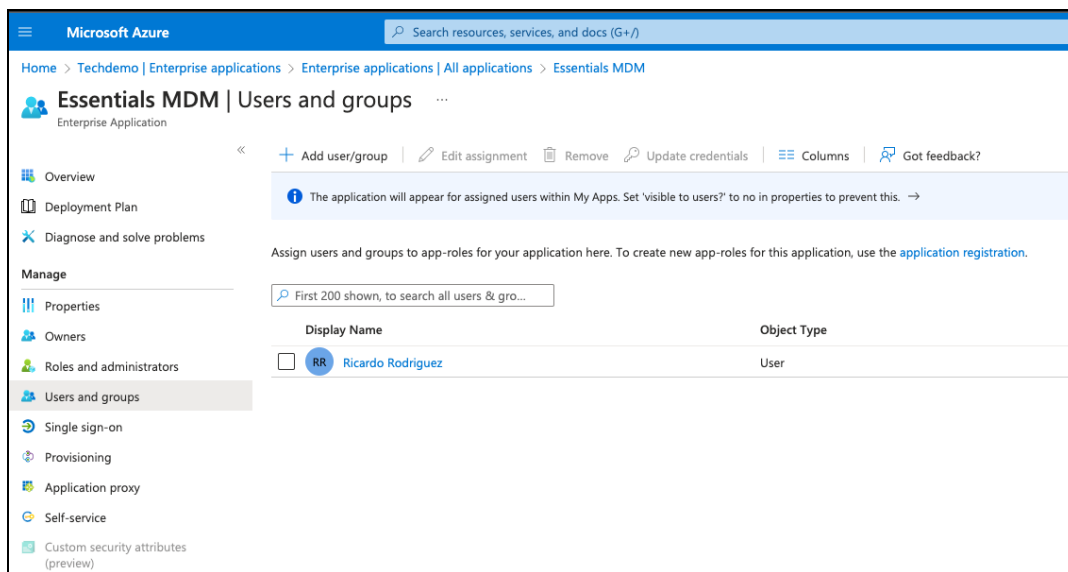
Name	<input type="text" value="nameidentifier"/>
Namespace	<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"/>
^ Choose name identifier format	
<input type="text" value="Windows domain qualified name"/>	
Source *	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation
Source attribute *	<input type="text" value="user.userprincipalname"/>

Save changes and close this section.

8. Next, in the SAML Certificate section, download Certificate (Base64). It will serve as cert X509 in Essentials SAML settings.

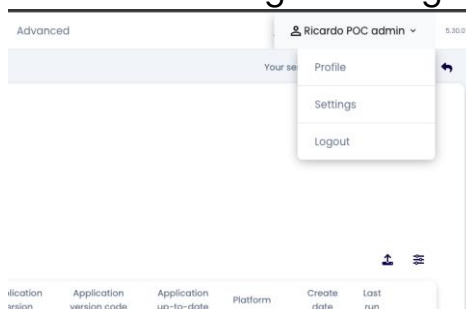
SAML Signing Certificate		Edit
Status	Active	
Thumbprint	865AD531EB41B808EA24C626B71EB35E36CC3241	
Expiration	3/29/2024, 3:31:32 PM	
Notification Email	mike.ross@therealfamoc.onmicrosoft.com	
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/d6e0ffb0-2987- ..."/>	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

It should also be remembered that users and / or groups of users who will be able to log in using this method must be assigned to the application. To do this, go to the Users and groups section and then click Add user/group.

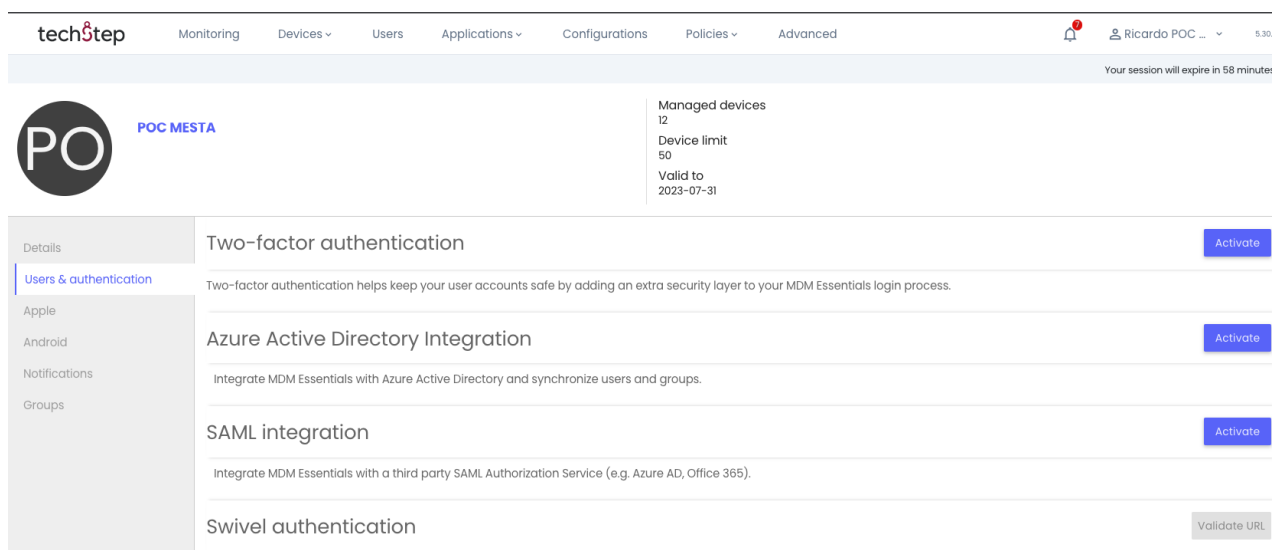


SAML configuration in Essentials MDM

To configure SAML Azure in Essentials navigate to organization settings:



1. Then, find the SAML integration under “Users and authentication” section and click Activate.



2. Upload the previously downloaded Certificate (Base64).
3. Enter the same Entity ID you entered in Azure portal.
4. For Login URL enter User access URL from the Azure portal. From this page you can also log in to FAMOC.

Properly edited data looks like this:

The screenshot shows the 'SAML settings' window with a progress bar at the top indicating three steps: 'Provide credentials' (active), 'User creation', and 'User fields mapping'. The 'Provide credentials' section contains three input fields: 'Login URL *' with the value 'https://login.microsoftonline.com/ed66d488-3c7d-4237-842e-ae8344c50123/saml2', 'Entity ID *' with the value 'https://test.techstep.com', and 'X.509 Certificate *' with a selected file 'Essentials MDM (1).cer (1.066 kB)'. A 'Next' button is located at the bottom right.

Press "Next".

On the next page turn on "Auto-create" users and assign a Role for these Users. Press "Next".

On the last page you have to map the Essential MDM login (FAMOC login) to the correct SAML attribute. You can add more attributes. They are used to map attributes from Azure AD to Essentials MDM. Attribute mapping allows you to automatically create a user in Essentials MDM with the same data as in Azure AD. Thanks to this, the user can automatically have assigned values such as an email address or domain, which will allow for easier configuration, for example, an email account.

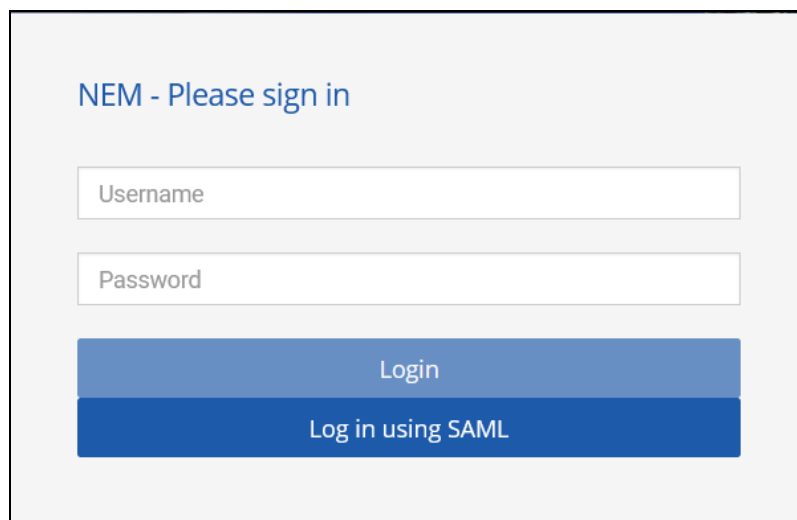
The screenshot shows the 'SAML settings' window with the progress bar now at the 'User fields mapping' step. It displays a table for mapping attributes. The first row maps 'FAMOC login *' (MDM Essentials attribute) to 'user:principalname' (SAML attribute). The second row has 'MDM Essentials attribute' selected in the first column and is currently empty in the second column. An 'Add new field' button is at the bottom of the table. 'Back' and 'Save settings' buttons are at the bottom right.

Known issues

In some cases, when you try to log in to Essentials MDM using Azure AD, you may receive an error 400. This can happen if you are already logged in to the same browser. To prevent this from happening, please log out and clear your browser cookies.

Summary

From now on, when logging in from the same computer and the same browser, it will be remembered that you have logged in with Azure AD and it will be suggested after entering the Essentials MDM login page.



The screenshot shows a login interface for 'NEM - Please sign in'. It features two input fields: 'Username' and 'Password'. Below these fields are two buttons: a light blue 'Login' button and a dark blue 'Log in using SAML' button.