# techŜtep

## 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 <u>https://portal.azure.com</u>.
- 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.

■ Microsoft Azure		Þ.	Ŗ	Q	?	ନ୍ଦ
Home > Techdemo   Enterprise applicati	ons > Enterprise applications					
Enterprise application	ons   All applications					
*	🕂 New application 💍 Refresh 🞍 Download (Export) 🛛 🚺 Preview info 📔 🎫 Columns 🛛 🐻 Preview features 🛛 🖗 Got feedback?					
Overview						
i Overview	View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.					
🗙 Diagnose and solve problems	The list of applications that are maintained by your organization are in application registrations.					
Manage	P Search by application name or object ID Application type == Enterprise Applications × Application ID starts with × <sup>+</sup> √ Add filters					
All applications	47 applications found					

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

=	Microsoft Azure	≫ Search resources, services, and docs (G+)	)	🛛 🖓 🗘 🍥 🕐 🖉 тесноемо (тесноемо.но)
Hom	e > Techdemo   Enterprise applications > Er	nterprise applications   All applications >		Create your own application ×
Bro	wse Azure AD Gallery			
				₽ Got feedback?
The A apps.	Create your own application 🔗 Got feedb zure AD App Gallery is a catalog of thousands of Browse or create your own application here. If yo	ack? f apps that make it easy to deploy and configure single sign ou are wanting to publish an application you have develope	on (SSO) and automated user provisioning. When deploying an app from d into the Azure AD Gallery for other organizations to discover and use, yo	If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.
				What's the name of your app?
<u>)</u> s	earch application	Single Sign-on : All User Account Management : .	All Categories : All	Input name
Clou	d platforms			What are you looking to do with your application?
				Configure Application Proxy for secure remote access to an on-premises application
	Amazon Web Services (AWS)	Google Cloud Platform	Oracle	<ul> <li>Register an application to integrate with Azure AD (App you're developing)</li> </ul>
				<ul> <li>Integrate any other application you don't find in the gallery (Non-gallery)</li> </ul>

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

⇒ FAMOC Venice | Single sign-on

Overview	Select a	a single sign-on method	Help me decide			
Deployment Plan      Manage      Properties      Owners      Roles and administrators (Pre	$\bigcirc$	Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.	<i>с</i> 3	SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.	A	Password-based Password storage and replay using a web browser extension or mobile app.
Users and groups     Single sign-on   Provisioning  Application proxy  Self-service  Security	ତ	Linked Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.				

#### 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): <u>https://serveradress.com/ui/</u> (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

https://venice.fancyfon.com/ui/

Reply URL (Assertion Consumer Service URL) \* 
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://venice.fancyfon.com/ui/

Intus://venice.fancyfon.com/ui/
Intus://venice.f

Save changes and close this section.

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	nameidentifier	
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	
∧ Choose name identifier format		
Windows domain qualified name		$\sim$
Source *	Attribute      Transformation	
Source attribute *	user.userprincipalname	$\sim$

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	https://login.microsoftonline.com/d6e0ffb0-2987
Certificate (Base64)	Download
Certificate (Raw)	Bownload
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.

		vices, and docs (G+/)
Home > Techdemo   Enterpris	se applications > Enterprise applications   All application	s > Essentials MDM
Essentials MD Enterprise Application	M   Users and groups	
	Add user/group   2 Edit assignment	🗊 Remove 🔑 Update credentials 📔 🎫 Columns 🕴 🖗 Got feedback?
Overview		
Deployment Plan	The application will appear for assigned use	rs within My Apps. Set 'visible to users?' to no in properties to prevent this. $ ightarrow$
🔀 Diagnose and solve problem	ns Assign users and groups to app-roles for your #	application here. To create new app-roles for this application, use the application registration.
Manage		
Properties	P First 200 shown, to search all users & gro	
A Owners	Display Name	Object Type
& Roles and administrators	RR Ricardo Rodriguez	User
Users and groups		
Single sign-on		
Provisioning		
Application proxy		
Self-service		
<ul> <li>Custom security attributes (preview)</li> </ul>		

#### **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.

tech <mark>Ŝ</mark> tep	Monitoring Devices - Users Applications - Configurations Policies - Advanced	📌 😩 Ricardo POC 👻 5.30.0
		Your session will expire in 58 minutes.
PO POCT	MESTA Managed devices 12 Device limit 50 Valid to 2023-07-31	
Details	Two-factor authentication	Activate
Users & authentication	Two-factor authentication helps keep your user accounts safe by adding an extra security layer to your MDM Essentials login proces	35.
Apple Android	Azure Active Directory Integration	Activate
Notifications	Integrate MDM Essentials with Azure Active Directory and synchronize users and groups.	
Groups	SAML integration	Activate
	Integrate MDM Essentials with a third party SAML Authorization Service (e.g. Azure AD, Office 365).	
	Swivel authentication	Validate URL

- 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:

	SAML settings	
Provide credentials	User creation	User fields mapping
⊂ Login URL *		
https://login.microsoftonline.com/ed6	6d488-3c7d-4237-842e-ae8344c50123/saml2	
https://test.techstep.com		
X 509 Cartificate *		
X.500 Continente		

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.

	SAML settings		×
Provide credentials	User creation	User fields mapping	
MDM Essentials attribute	SAML attribute		
FAMOC login *	* user userprincipalname	×	
MDM Essentials attribute	SAML attribute *	×	
	Add new field		
		Back	Save settings

#### **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.

NEM - Please	e sign in	
Username		
Password		
	Login	
	Log in using SAML	