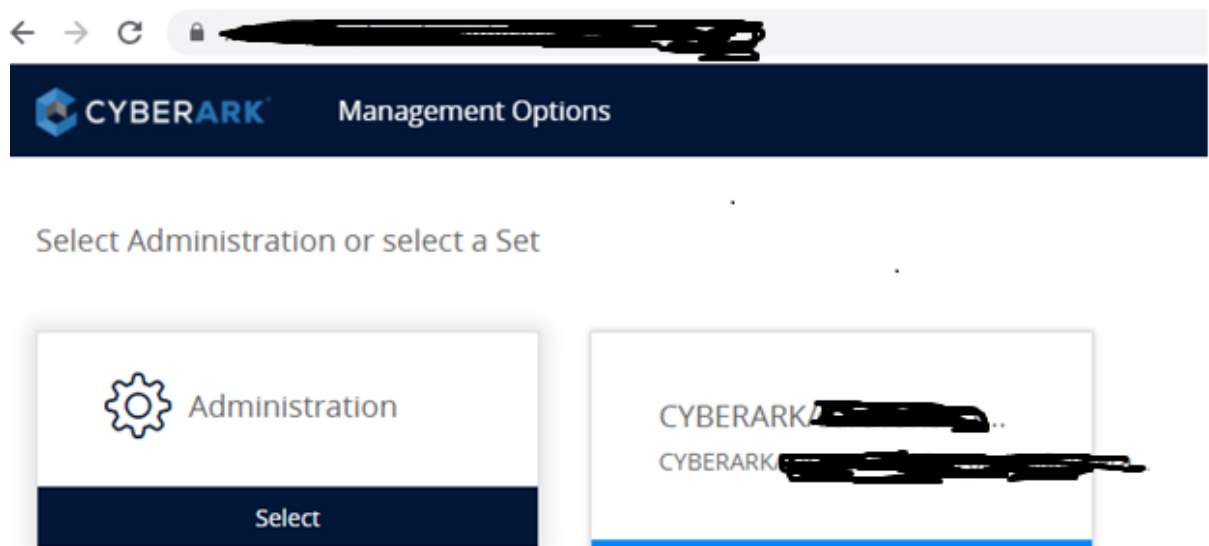


Enabling SAML Integration with Azure AD for EPM SaaS

1: Pre-requisites on CyberArk EPM

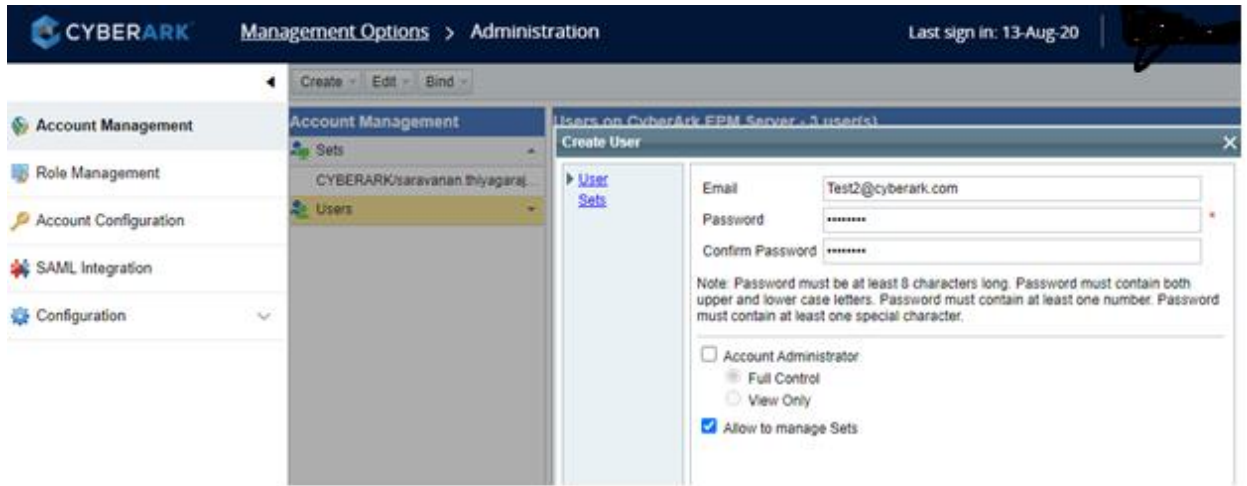
- 1.1 Login in to your EPM SaaS Admin Console as Administrator and Select Administration tab on the landing page. For example - Customers who had selected or chosen their Datacenter to be "US" will have received the link as "<https://login.epm.cyberark.com/login>". The Admin Console Link may vary depending upon the region you had selected during the Registration/Enrollment Process.



- 1.2 Select "Administration" tile and Under Account Management, please make sure to import/create other Administrators User Account (who will manage the EPM Policies) , View/Read only Accounts, leveraging email id and grant them require permission as "Account Administrator" or "Allow to manage sets".

The accounts that are created in EPM, will get authenticated thru Single Sign on and MFA .

Remember the Account that you had logon is "Super User " Account and as a Best Practices we encourage try not to use this account besides Setting up initial configurations such as
1)Create another admin account

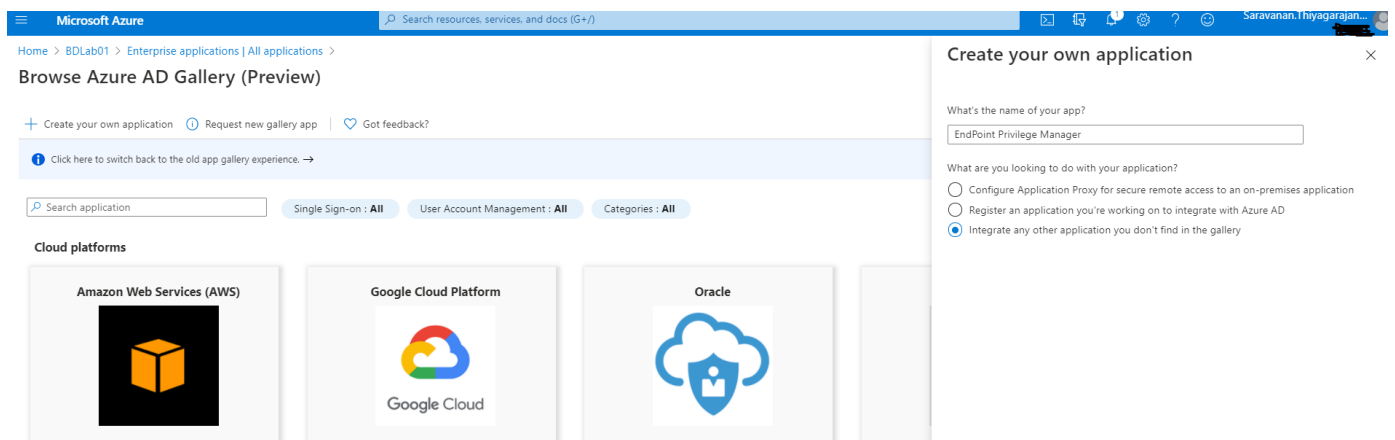


2: Configuration Steps in Azure AD to onboard EPM Application

2.1 Please login to Azure Portal Management console with Admin Access and select Azure Active Directory. Under “Manage” please select “Enterprise Applications” → New Application → Create your own Application →

Provide name : “<CyberArk EndPoint Privilege Manager>”

Choose Integrate any other application you don’t find in the gallery and click create



2.2 Under Manage click “Single Sign on” and select “SAML”

[Home](#) > [BDLab01](#) > [Enterprise applications | All applications](#) > [Browse Azure AD Gallery \(Preview\)](#) > [EndPoint Privilege Manager | Single sign-on](#) >

EndPoint Privilege Manager | SAML-based Sign-on

Enterprise Application

The screenshot shows the Azure AD portal interface for configuring SAML-based sign-on for the EndPoint Privilege Manager application. The left-hand navigation pane is expanded to the 'Manage' section, with 'Single sign-on' selected. The main content area is titled 'Set up Single Sign-On with SAML' and includes a link to the configuration guide. It contains three numbered sections: 1. Basic SAML Configuration, 2. User Attributes & Claims, and 3. SAML Signing Certificate. The 'Basic SAML Configuration' section lists fields like Identifier (Entity ID), Reply URL, Sign on URL, Relay State, and Logout URL, with their respective requirements. The 'User Attributes & Claims' section shows a mapping of user attributes to claims. The 'SAML Signing Certificate' section indicates that no certificates exist for this application.

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs

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

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating EndPoint Privilege Manager.

- 1** Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout URL	Optional
- 2** User Attributes & Claims [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- 3** SAML Signing Certificate

No certificates exist for this application. [Add a certificate](#)

2.3 Make the following changes in the “Setup Single Sign On with SAML”.

Basic SAML Configuration

- Edit

Identifier (Entity ID)

<https://login.epm.cyberark.com/SAML>

Reply URL (Assertion Consumer Service URL)

<https://login.epm.cyberark.com/SAML/acsu>

Sign on URL

<https://login.epm.cyberark.com/SAML/<Your Org name >>

Relay State

Optional

Logout Url

<https://login.epm.cyberark.com/SAML/slo>

and Click “Save”.

Home > BDLab01 > Enterprise applications | All applications > EndPoint Privilege Manager | Single sign-on >

EndPoint Privilege Manager | SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Privileged sessions (Preview)

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating EndPoint Privilege Manager.

- Basic SAML Configuration**
 - Identifier (Entity ID) **Required**
 - Reply URL (Assertion Consumer Service URL) **Required**
 - Sign on URL **Optional**
 - Relay State **Optional**
 - Logout Url **Optional**
- User Attributes & Claims
 - givenname user.givenname
 - surname user.surname
 - emailaddress user.mail
 - name user.userprincipalname
 - Unique User Identifier user.userprincipalname
- SAML Signing Certificate
 - No certificates exist for this application. [Add a certificate](#)
- Set up EndPoint Privilege Manager
 - You'll need to configure the application to link with Azure AD.

Basic SAML Configuration

Save

Identifier (Entity ID) * ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

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

Default

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

2.4 After you click save , your page gets refreshed with certificate and other values as below.

EPMSSO | SAML-based Sign-on

Enterprise Application

The screenshot shows the configuration page for EPMSSO SAML-based Sign-on. The left sidebar contains navigation links: Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service), and Security (Conditional Access, Permissions, Token encryption). The main content area has tabs: Upload metadata file, Change single sign-on mode, Test this application, and Got feedback?. The 'SAML Signing Certificate' section (step 3) shows a table with details: Status (Active), Thumbprint (7910942A288737CD9AD978EF89E29CDF590AD24), Expiration (8/19/2023, 10:46:18 AM), Notification Email (Saravanan.Thiyagarajan@cyberark.com), App Federation Metadata Url (https://login.microsoftonline.com/9fba08a7-ca98-...), Certificate (Base64) (Download), Certificate (Raw) (Download), and Federation Metadata XML (Download). The 'Set up EPMSSO' section (step 4) provides instructions to configure the application to link with Azure AD, listing Login URL, Azure AD Identifier, and Logout URL, each with a corresponding URL and a download icon. A link to 'View step-by-step instructions' is also present.

SAML Signing Certificate	
Status	Active
Thumbprint	7910942A288737CD9AD978EF89E29CDF590AD24
Expiration	8/19/2023, 10:46:18 AM
Notification Email	Saravanan.Thiyagarajan@cyberark.com
App Federation Metadata Url	https://login.microsoftonline.com/9fba08a7-ca98-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Set up EPMSSO

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

Login URL	https://login.microsoftonline.com/9fba08a7-ca98-...
Azure AD Identifier	https://sts.windows.net/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/
Logout URL	https://login.microsoftonline.com/common/wsrfederation?wa=wsignout1.0

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

2.5 Download the Certificate to your local machine and copy the following values. Or follow the view step by step instructions.

- **SAML Single Sign-On Service URL:** <https://login.microsoftonline.com/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/saml2>
- **SAML Entity ID:** <https://sts.windows.net/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/>
- **Sign-Out URL:** <https://login.microsoftonline.com/common/wsrfederation?wa=wsignout1.0>

2.6 Under Manage → Users and groups → Add user

Please add the users or groups who want to access the EndPoint Privilege Manager.

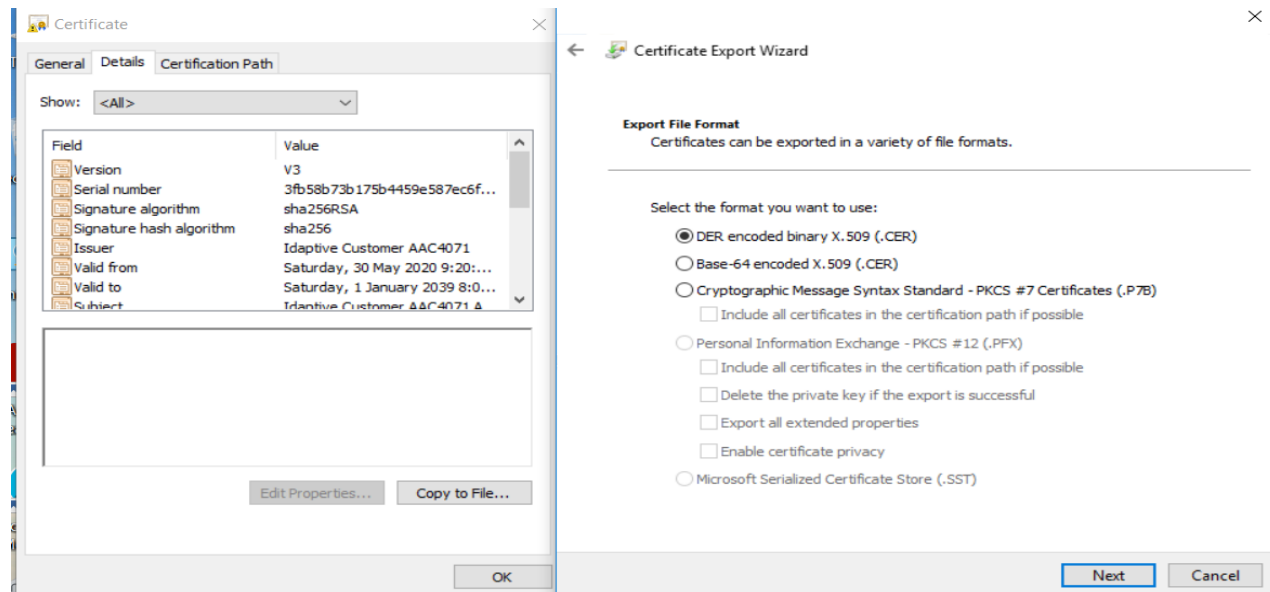
3. Configuration Steps in CyberArk EPM AdminConsole

3.1 Login in to your EPM SaaS Admin Console as Administrator and select “Administration” tile and Choose “SAML Integration” and edit the configuration as follows. Following values are required to complete the setup and receive them from Azure AD

following thru the Section 2.

IDP Issuer URL	https://sts.windows.net/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/
IDP Server Certificate	<Upload the certificate obtained from IDP>
IDP Single Sign On UR	https://login.microsoftonline.com/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/saml2
IDP Single Logout URL	https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

Note: Please make sure to convert the certificate to “.der” format using your prefer tool For example – openssl



3.2 EPM Login Configuration

Organization Identifier : <Your Org name or customize name >

EPM Login URL : <https://login.epm.cyberark.com/SAML/<Organization Identifier>>

Lock EPM login URL for users and redirect to IDP authentication – Please refer to below image

EPM Logout URL : <<https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0>>

IDP Server Configuration

Properties

Property	Value
Signed Authentication Request	True
Signed Login Request	True
Signed Assertion	True
Encrypted Assertion	False
Signed SAML Response	False
Signed Logout Response	False

IDP Issuer URL	https://sts.windows.net/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/ Value is case-sensitive
IDP Server Certificate	Uploaded Browse CER file in DER encoded binary X.509 format
IDP Single Sign On URL	https://login.microsoftonline.com/9fba08a7-ca98-4bf5-84a6-8da7f0f214a8/saml2 IDP Server URL where EPM sends the SAML request for the login
IDP Single Logout URL	https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 IDP Server URL where EPM sends the SAML request for the logout

EPM Login Configuration

Organization Identifier	st A segment that is added to the EPM service provider Entity ID and turns it into a unique EPM login URL for your organization. Value is case-sensitive. The recommended value is your organization shorten name or abbreviation.
EPM Login URL	https://login.epm.cyberark.com/SAML/st URL where user can login to EPM server
Lock EPM login URL for users and redirect to IDP authentication	
☐ All Users	
☒ All users, beside Account Admin	
☐ None	
EPM Logout URL	https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 URL where user is redirected upon logout. This must not be the EPM login URL.

5)Click Save

Validation Step:

After above steps are completed, You should still able to login to EPM Admin console with your default admin account without going thru Azure AD SSO.

Basically admin account is configured for "Local Authentication". All other accounts (Non-admin account) will go thru Azure AD Security.

If you prefer to enable SSO including your admin accounts, please choose "All users" under Lock EPM Login URL.