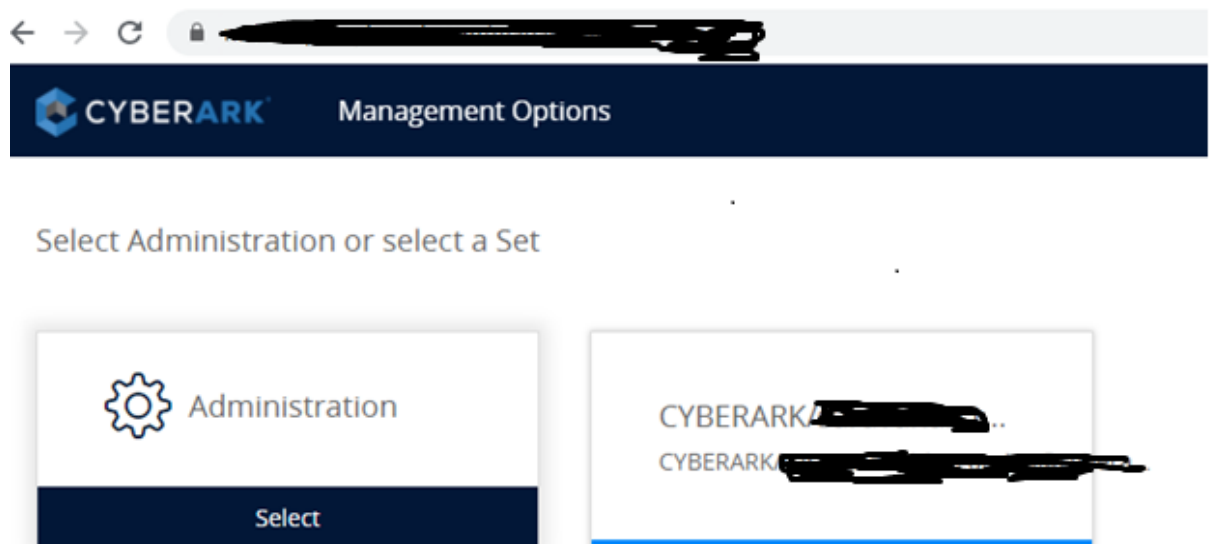


Enabling SSO and MFA for EPM with Duo.

1: Pre-requisites on EPM

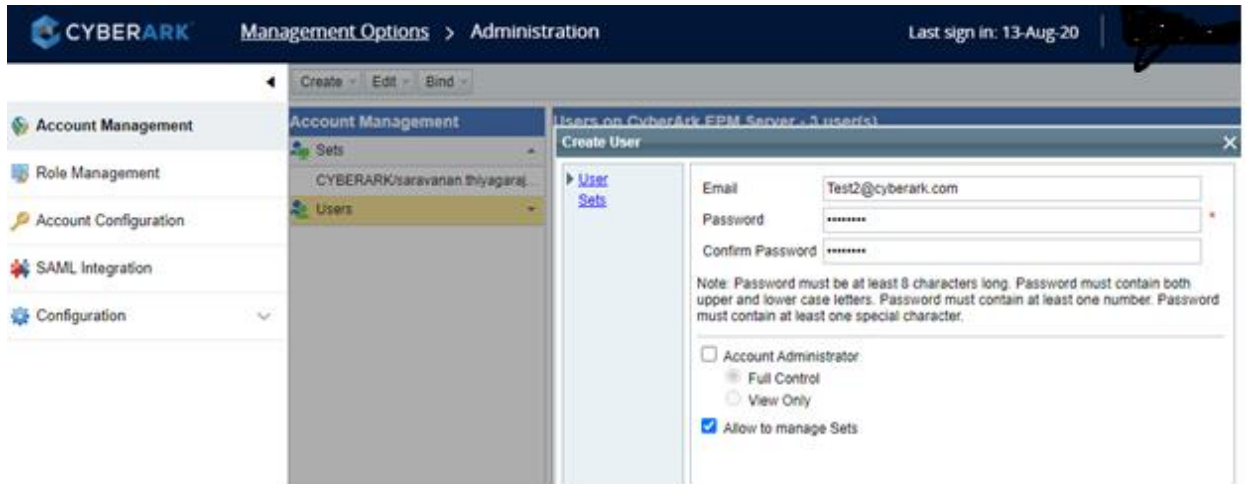
- 1.1 Login in to your EPM SaaS Admin Console as Administrator and Select Administration tab on the landing page. For example - Customers who had selected or chosen their Datacenter to be “US” will have received the link as “<https://login.epm.cyberark.com/login>”. The Admin Console Link may vary depending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

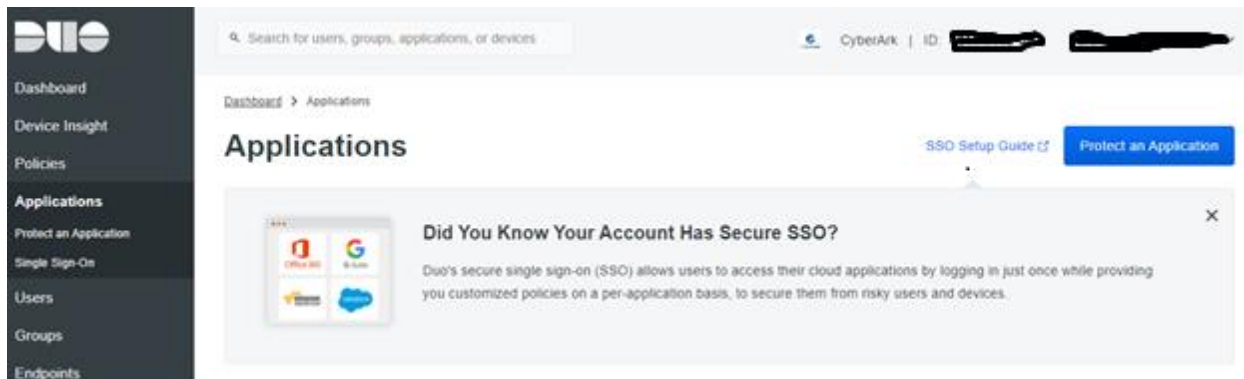
The accounts that are created in EPM, will get authenticated thru Single Sign on and MFA .

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

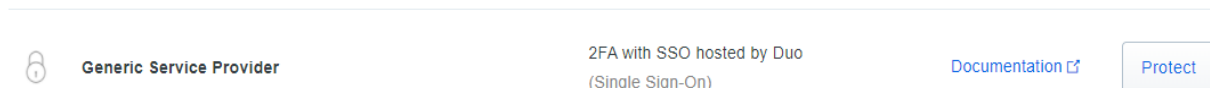


2: Configuration Steps in Duo to onboard EPM Application

2.1 Please login to Duo instances with Admin Rights and click Application menu



2.2 Click “Protect an Application” and search for “Generic” and choose the Generic Service Provider with SSO and click protect.



2.3 Under “Service Provider” please update the following values.

Service Provider Name	< EndPoint Privilege Manager>
Entity ID *	https://login.epm.cyberark.com/SAML
Assertion Consumer Service *	https://login.epm.cyberark.com/SAML/acsu
Single Logout URL	https://login.epm.cyberark.com/SAML/slo
Service Provider Login URL	< https://login.epm.cyberark.com/SAML/st>

Service Provider

Service provider name *

The name of the service provider being configured.

Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service *

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL

Optional: The service provider endpoint that receives and processes SAML logout requests.

Service Provider Login URL

Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Rest all default values and save.

2.4 Download the certificate from DuoSecurity , clicking the “Download Certificate” Button and store them locally to get upload in to EPM Console.

Reports

Settings

Need Help?

[Chat with Tech Support](#)

[Email Support](#)

Call us at 1-855-386-2884

Account ID

4211-1418-38

Deployment ID

[DUO58](#)

Helpful Links

[Documentation](#)

[User Guide](#)

[Knowledge Base](#)

Metadata URL

<https://330-100000000.330.duosecurity.com/saml2/sprn/>

Certificate Fingerprints

SHA-1 Fingerprint

DA:8F:59:8B:89:68:8F:7E:D0:7D:37:D7:DD:BF:69:13:0

SHA-256 Fingerprint

F4:53:4D:D7:F8:C0:49:BA:26:FA:CE:F0:D5:D7:80:D8:0

Downloads

Certificate

[Download certificate](#)



SAML Metadata

[Download XML](#)

Service Provider

3.Configuration Steps in 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 Duo following thru the Section 2.

IDP Issuer URL	https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/metadata
IDP Server Certificate	<Upload the certificate obtained from IDP>
IDP Single Sign On UR	https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/sso
IDP Single Logout URL	https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/slo

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 LogoutURL : <<https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/slo> >

IDP Issuer URL	https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/metadata	
	Value is case-sensitive	
IDP Server Certificate	Uploaded	Browse
	CER file in DER encoded binary X.509 format	
IDP Single Sign On URL	https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/sso	
	IDP Server URL where EPM sends the SAML request for the login	
IDP Single Logout URL	https://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/slo	
	IDP Server URL where EPM sends the SAML request for the logout	
EPM Login Configuration		
Organization Identifier		
	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://sso-fb00ecce.sso.duosecurity.com/saml2/sp/DINV7FKNW4O8UGVVE8EV/slo	

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 with out going thru DUO SSO. Basically admin account is configured for "Local Authentication". Basically all other accounts (Non-admin account) will go thru Duo Security.

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