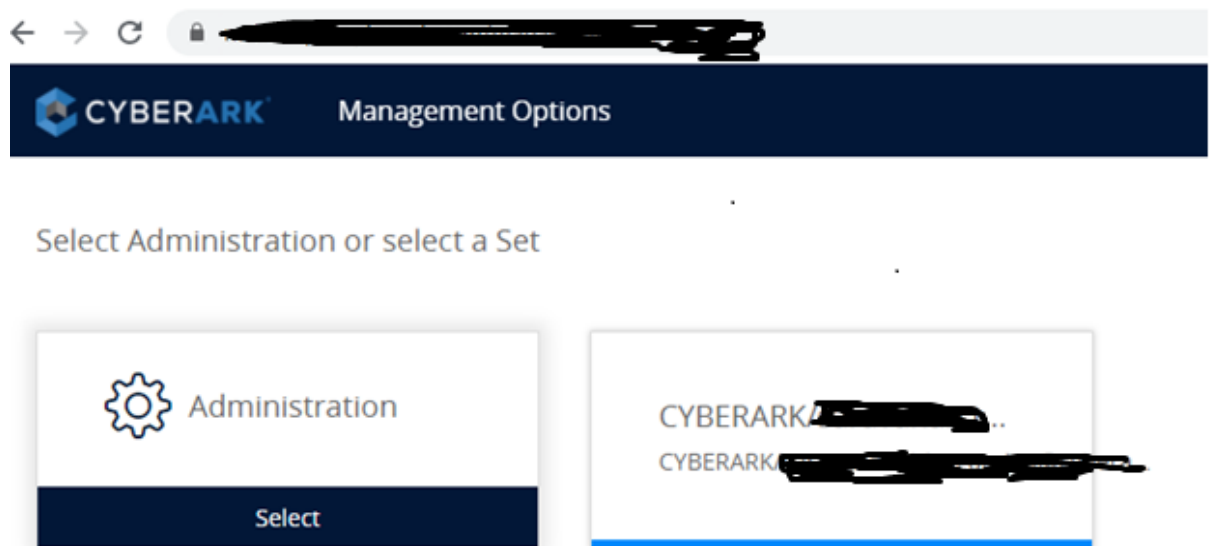


Enabling SAML Integration with OneLogin Identity for EPM SaaS

1: Pre-requisites on CyberArk EPM

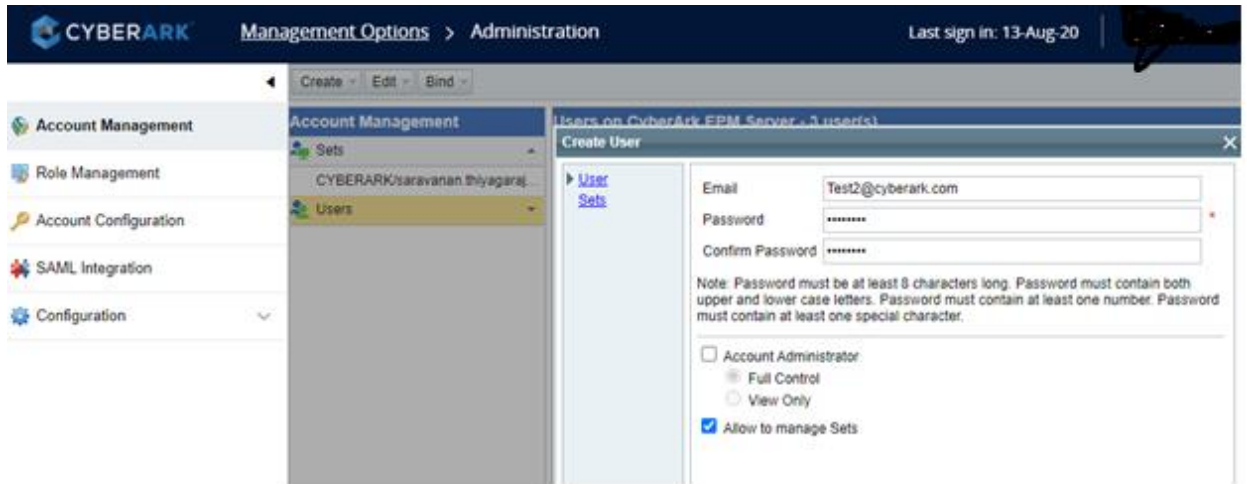
- 1.1 Login in to your EPM SaaS Admin Console as Administrator and Select Administration tab on the landing page. For example - Customers who had selected or chosen their Datacenter to be "US" will have received the link as "<https://login.epm.cyberark.com/login>". The Admin Console Link may vary depending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



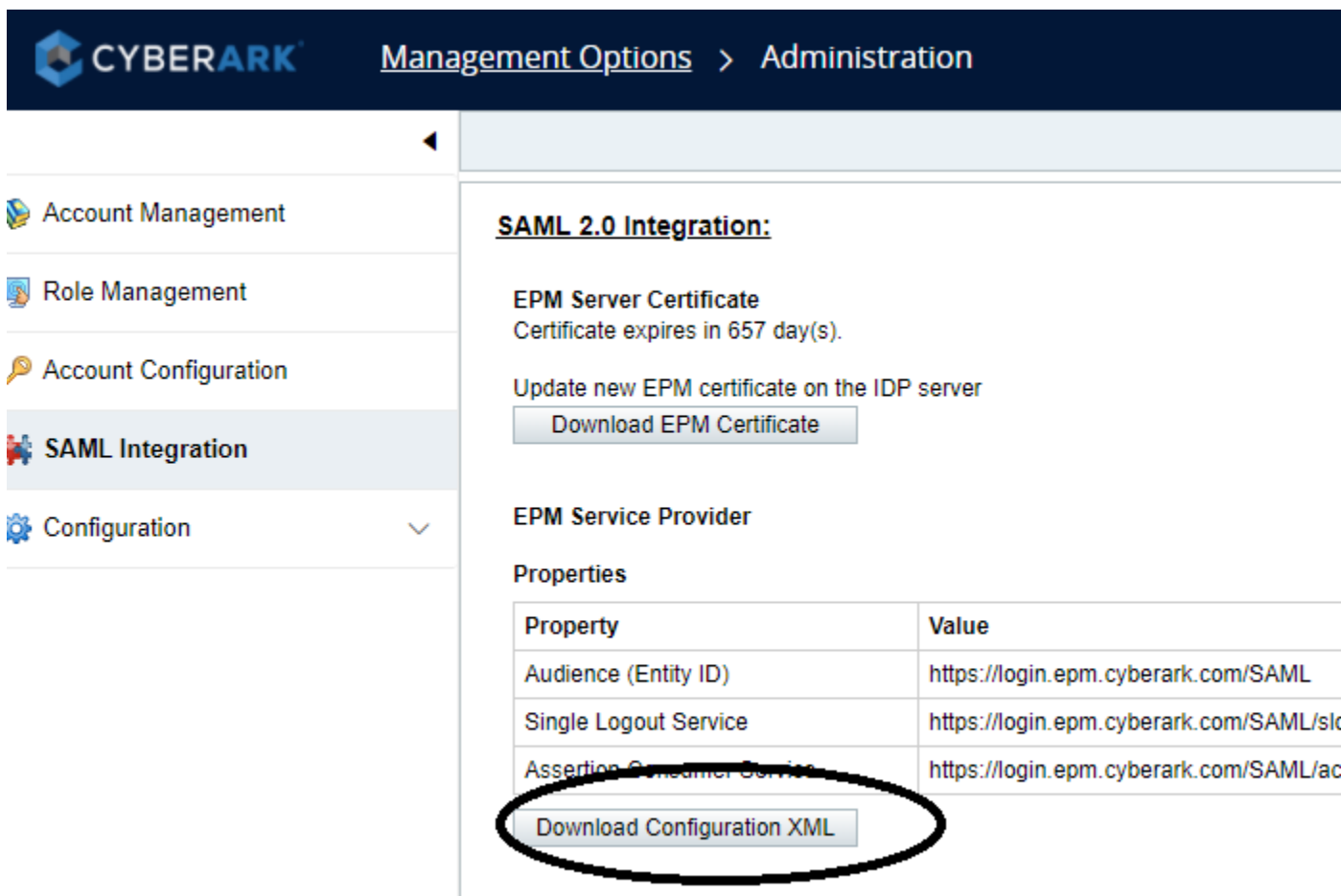
- 1.2 Select "Administration" tile and Under Account Management, please make sure to import/create other Administrators User Account (who will manage the EPM Policies) , View/Read only Accounts, leveraging email id and grant them require permission as "Account Administrator" or "Allow to manage sets".

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



1.3 Please make sure to download the XML (metadata) file and Certificate from the EPM Admin Console. Logon to the EPM Administrative console as “Administrator” and select “Administration” Icon and Click on the SAML Integration. Under “EPM Service Provider” please click “Download configuration XML” and store the xml file locally and upload them to the OneLogin (if require)



2: Configuration Steps in OneLogin to OnBoard CyberArk EPM SAML Application

Reference Link : https://elispostman.github.io/docs/v6/enterprise/sso/saml_onelogin

3.Configuration Steps in CyberArk EPM AdminConsole

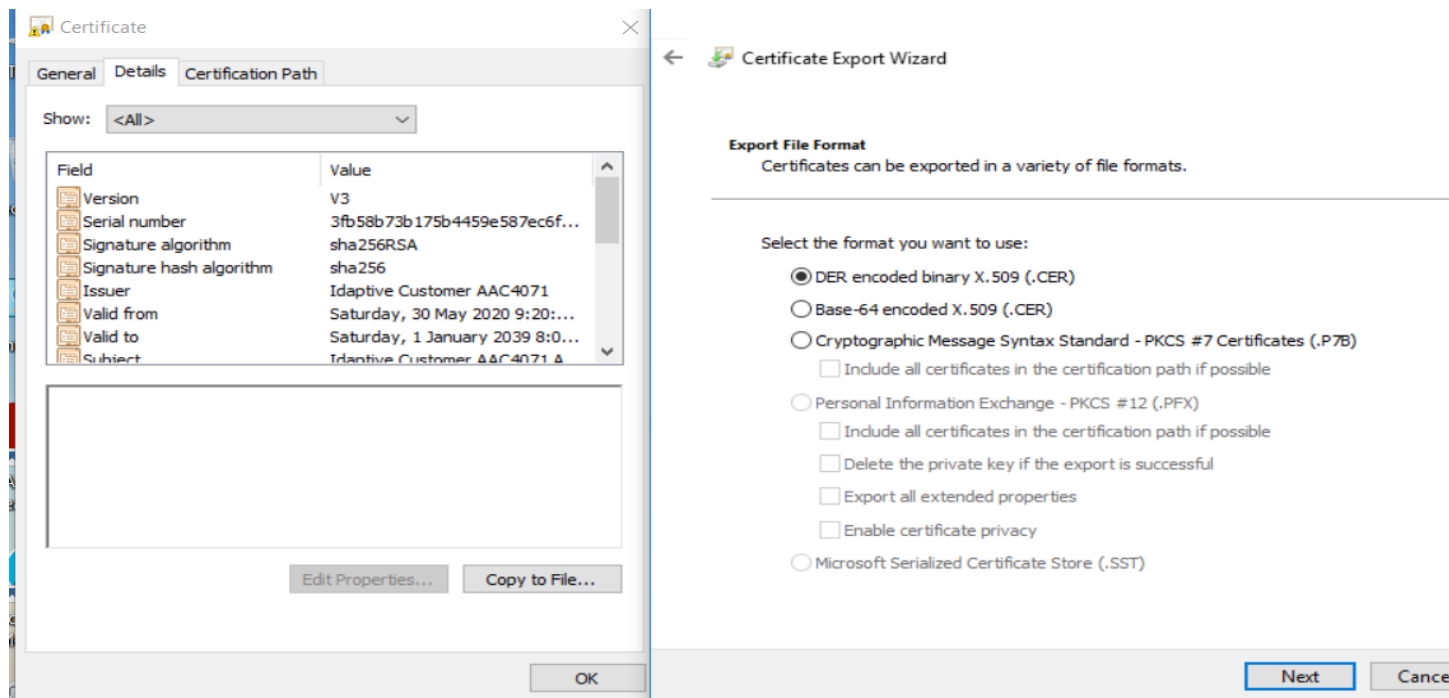
3.1 Login in to your EPM SaaS Admin Console as Administrator and select “Administration” tile and Choose “SAML Integration” and edit the configuration as follows.

Following values are required from OneLogin to complete the setup

IDP Issuer URL	Onelogin URL
IDP Server Certificate	<Upload the certificate that you had downloaded from OneLogin >
IDP Single Sign On URL	OneLogin SSO URL
IDP Single Logout URL	https://login.epm.cyberark.com/SAML/slo

Note: Please make sure to provide right values in to the IDP Single Sign on URL.

Note: Please make sure to convert the certificate to “.der” format using your prefer tool For example – <https://www.sslshopper.com/ssl-converter.html>



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.epm.cyberark.com/SAML/slo>>

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	

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 OneLogin.

Basically, admin account is configured for "Local Authentication". All other accounts (Non-admin account) will go thru Ping One.

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