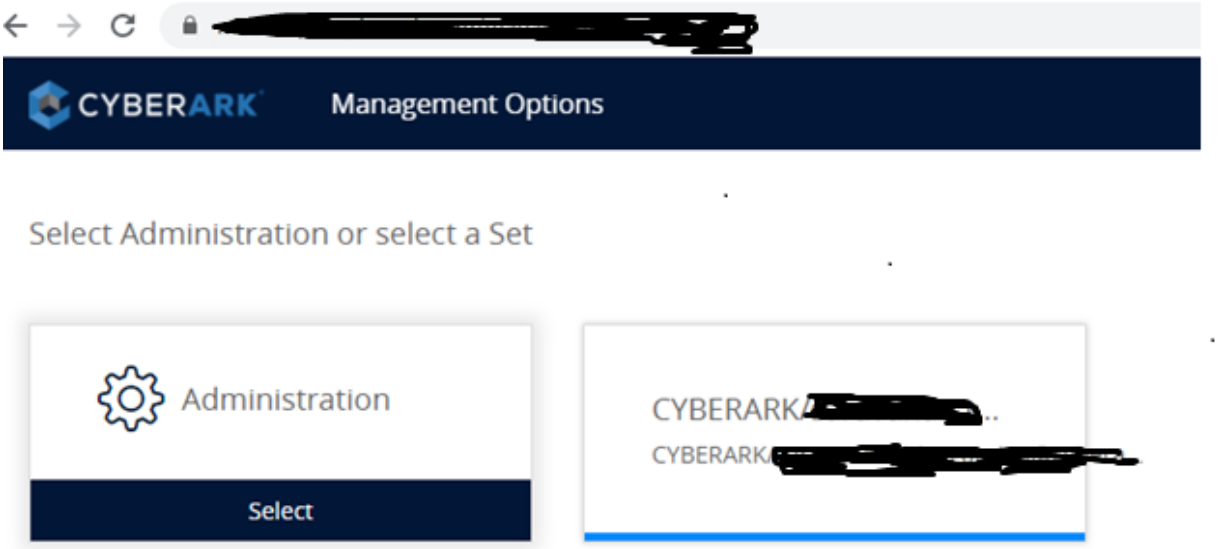
Enabling SAML Integration with Ping One Identity for EPM SaaS

1: Pre-requisites on CyberArk EPM

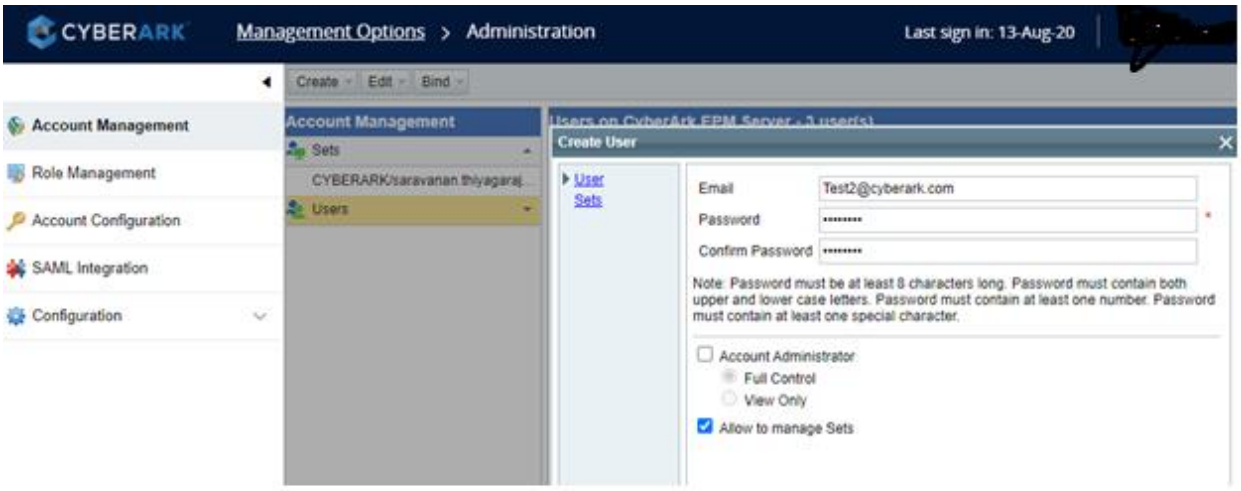
1.1 Login in to your EPM SaaS Admin Console as Administrator and Select Administration tab on the landing page. For example - Customers who had selected or chosen their Datacenter to be "US" will have received the link as "https://login.epm.cyberark.com/login" . The Admin Console Link may vary depending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



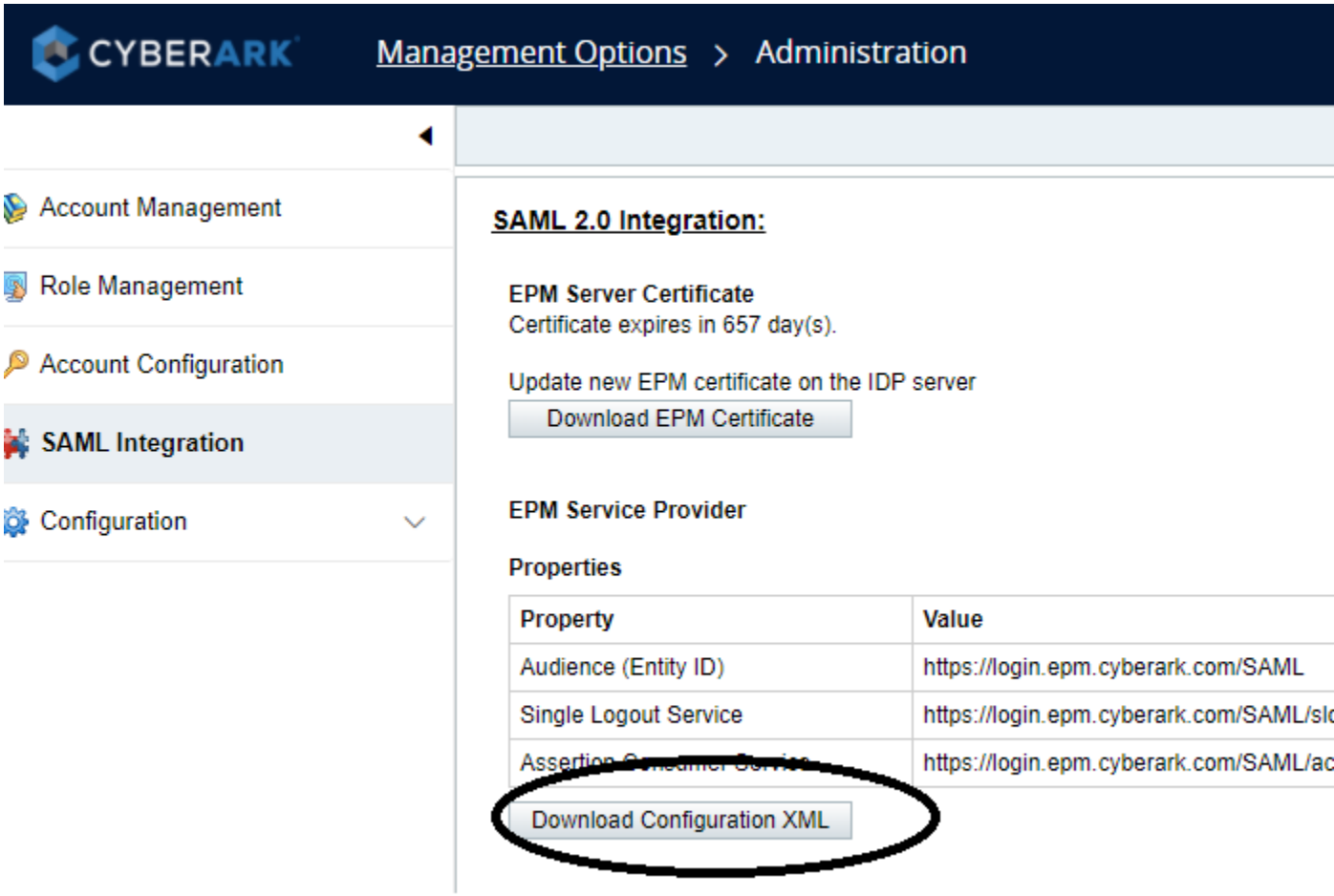
1.2 Select "Administration" tile and Under Account Management, please make sure to import/create other Administrators User Account (who will manage the EPM Policies) , View/Read only Accounts, leveraging email id and grant them require permission as "Account Administrator" or "Allow to manage sets".

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

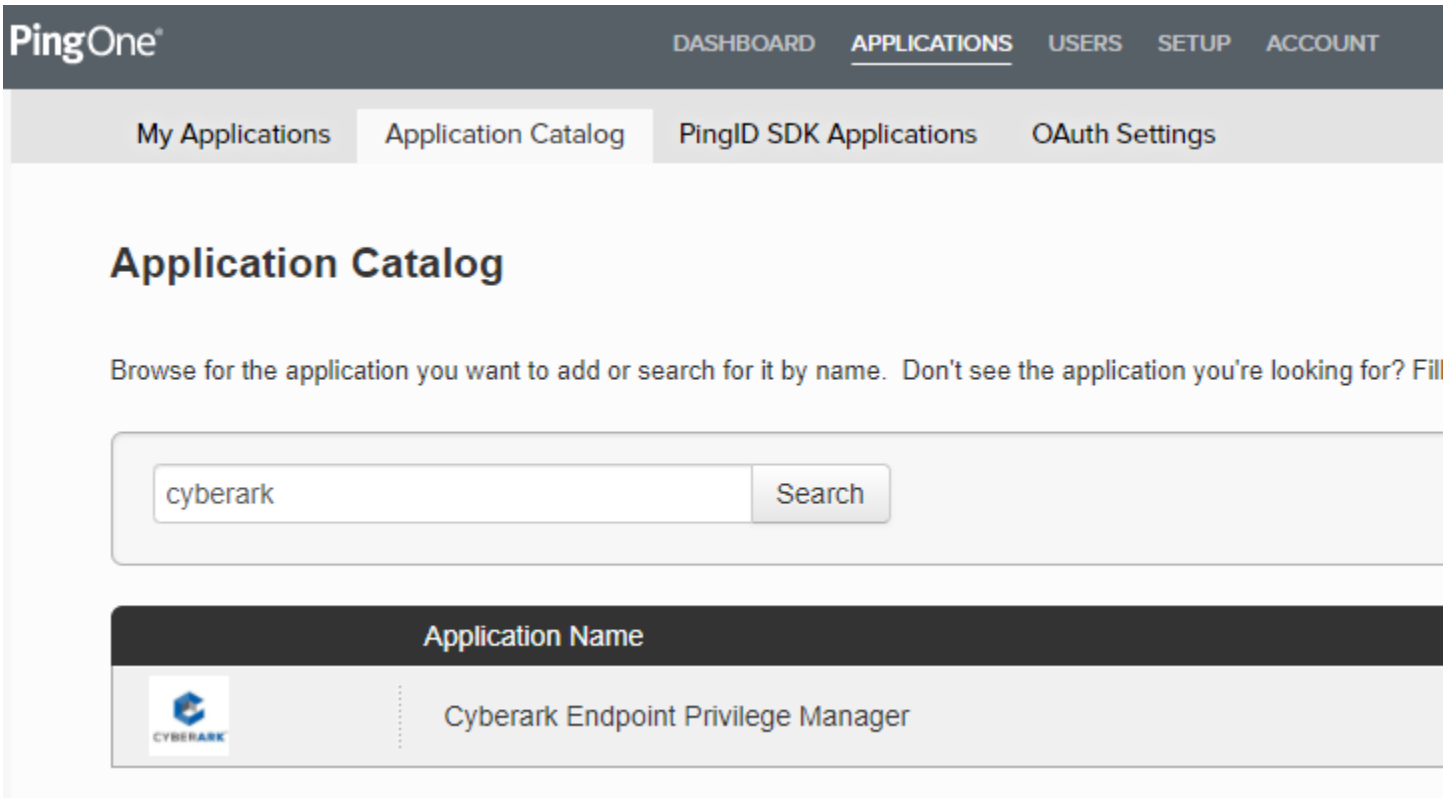


1.3 Please make sure to download the XML (metadata) file and Certificate from the EPM Admin Console. Logon to the EPM Administrative console as "Administrator" and select "Administration" Icon and Click on the SAML Integration. Under "**EPM Service Provider" please click "Download configuration XML"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



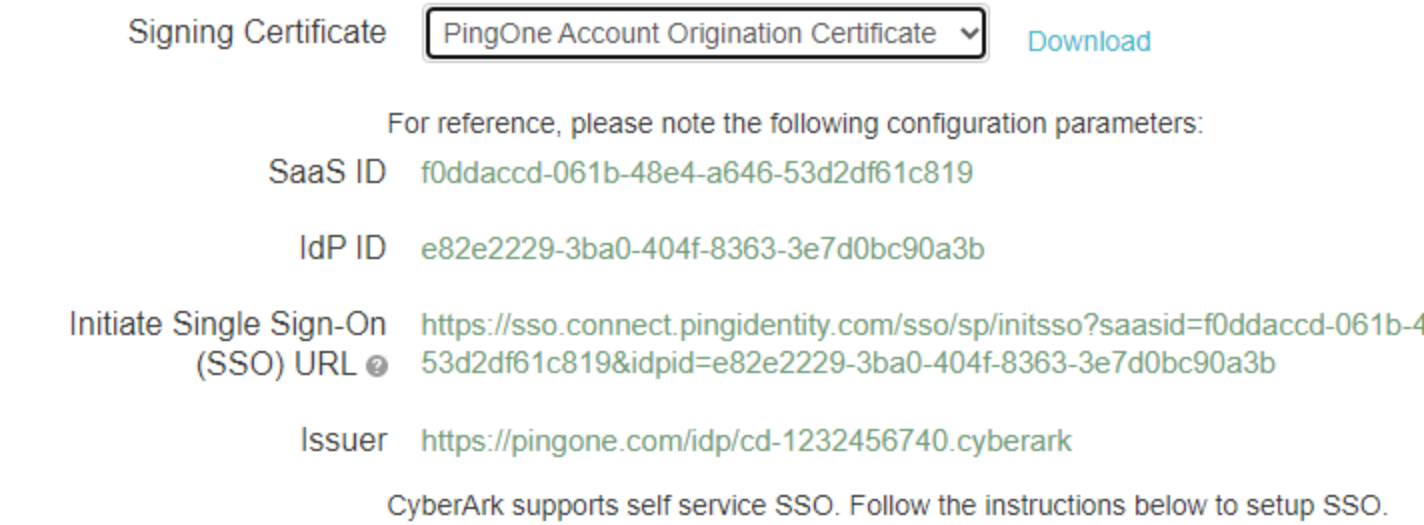
2: Configuration Steps in Ping One (IDP) to OnBoard CyberArk EPM SAML Application

2.1 Please logon to Ping Administrative Console and select “Application Catalog” and search for Cyberark. Please click the arrow and click the setup button.

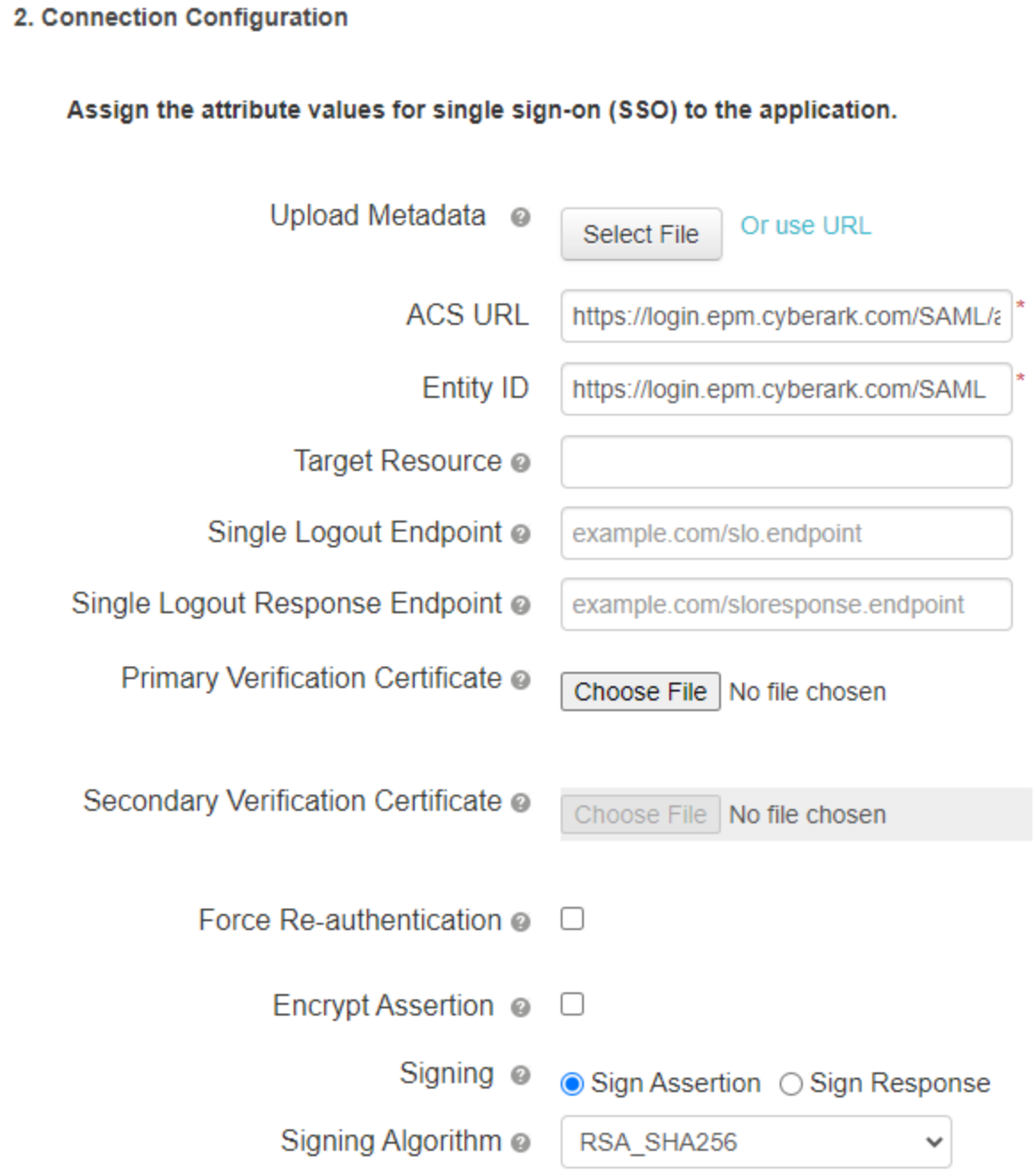


2.2 Under “SSO Instructions”

1. SSO Instructions



a) Download store the certificate locally.
b) Copy all the values and store them and click continue to Next step.



Please upload the Metadata xml file obtained from EPM Admin console (From step 1.3) to “Upload Metadata” and Upload the certificate to “Primary Verification Certificate” value.

If you prefer to configure Single Logout Endpoint, pl enter the value as https://login.epm.cyberark.com/SAML/slo

3.0 Attribute Mapping: Please select Email (work) and click continue to next.

3. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	SAML_SUBJECT *	Identifies the authenticated principal	SAML_SUBJECT ☐ As Literal Advanced
2	Email *	Email attribute (required)	Email (Work) ☐ As Literal Advanced

4.0 Assign the application (CyberArk End point Privilege Manager) to the specific group who will manage the application need, and review the setup and click Finish.

3.Configuration Steps in CyberArk EPM AdminConsole

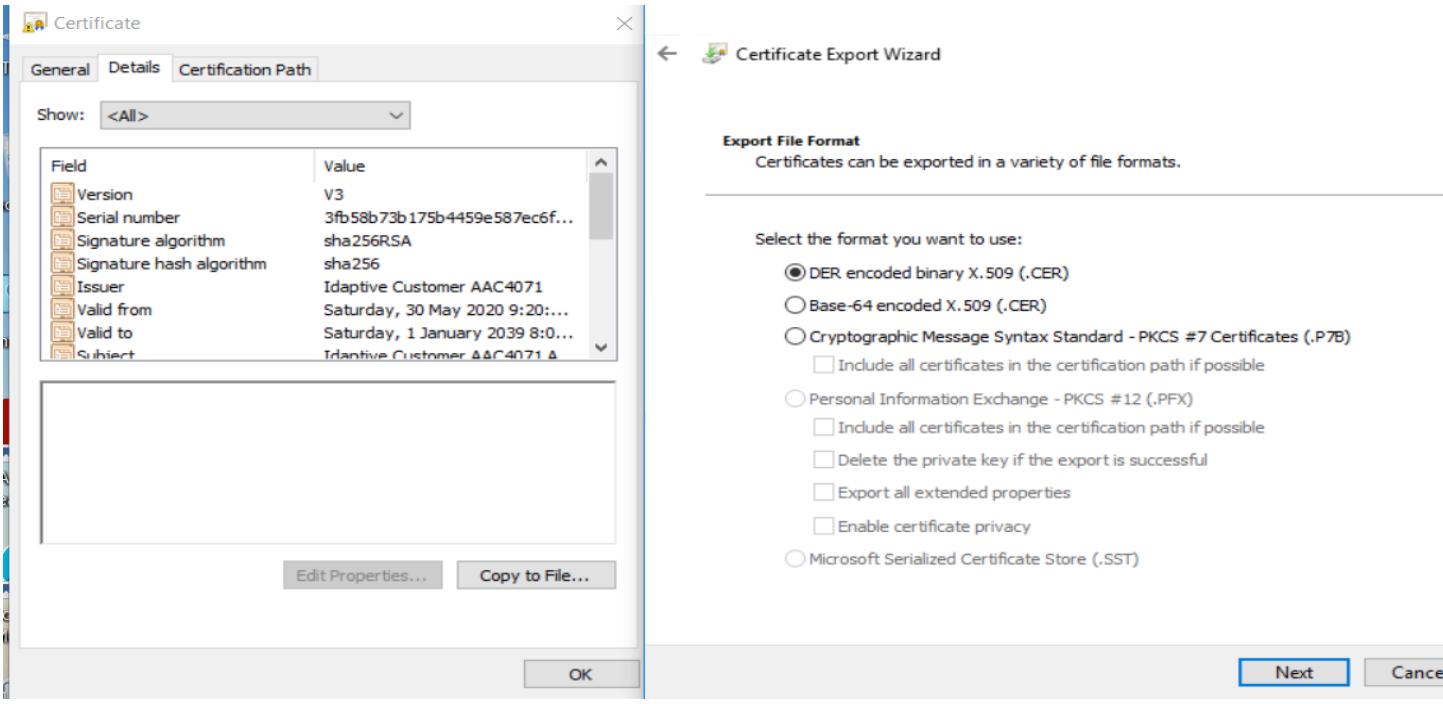
3.1 Login in to your EPM SaaS Admin Console as Administrator and select “Administration” tile and Choose “SAML Integration” and edit the configuration as follows.

Following values are required from Ping Identity to complete the setup

IDP Issuer URL	https://pingone.com/idp/<your ping tenant id>
IDP Server Certificate	<Upload the certificate that you had downloaded from Ping >
IDP Single Sign On URL	https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=69c36e39-72cf-4bbc-9aab-33b75be0cf4b
IDP Single Logout URL	https:// <Ping one logout end point>

Note : Please make sure to provide right values in to the IDP Single Sign on URL. The value of idpid is important and can be obtained from Ping Admin Console.

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



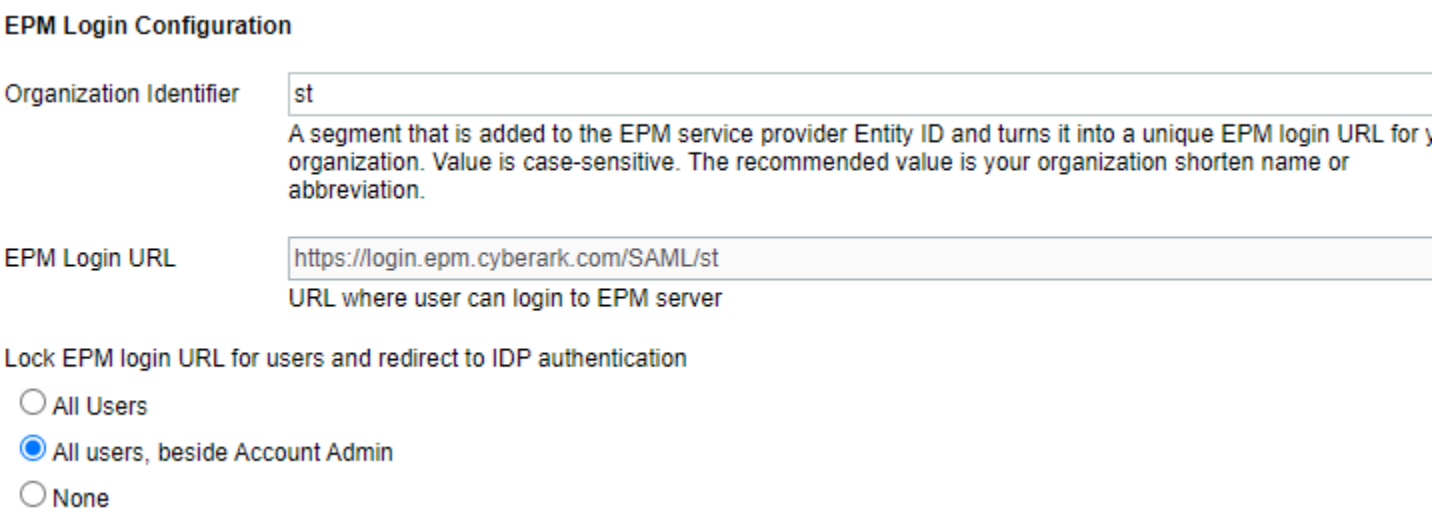
3.2 **EPM Login Configuration**

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.epm.cyberark.com/SAML/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 without going thru Ping One.
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.