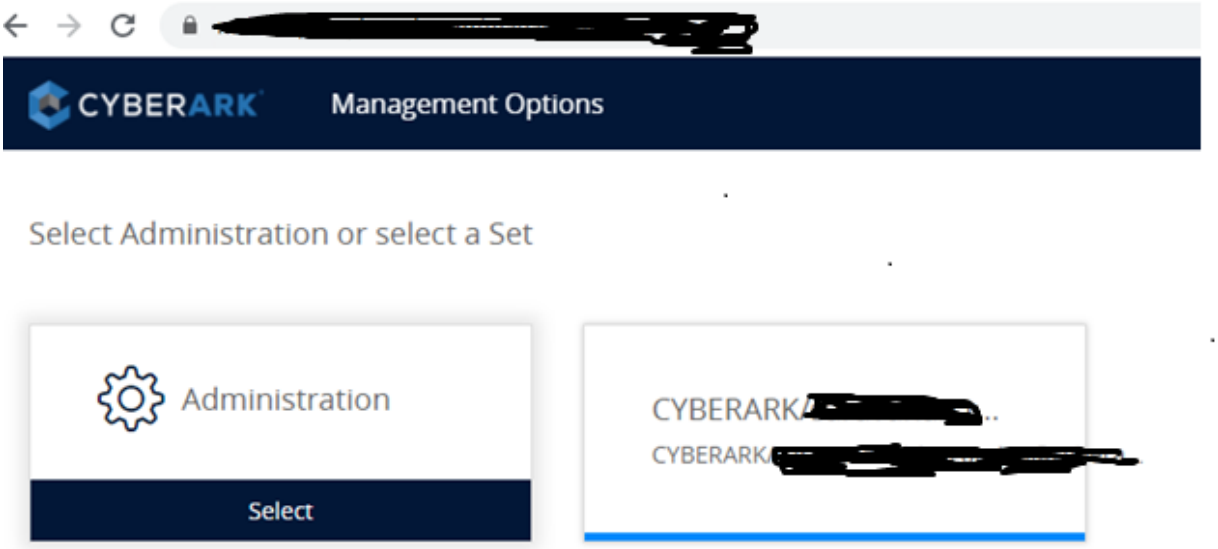
# Enabling SAML Integration with Okta Identity for EPM SaaS

## 1: Pre-requisites on CyberArk EPM

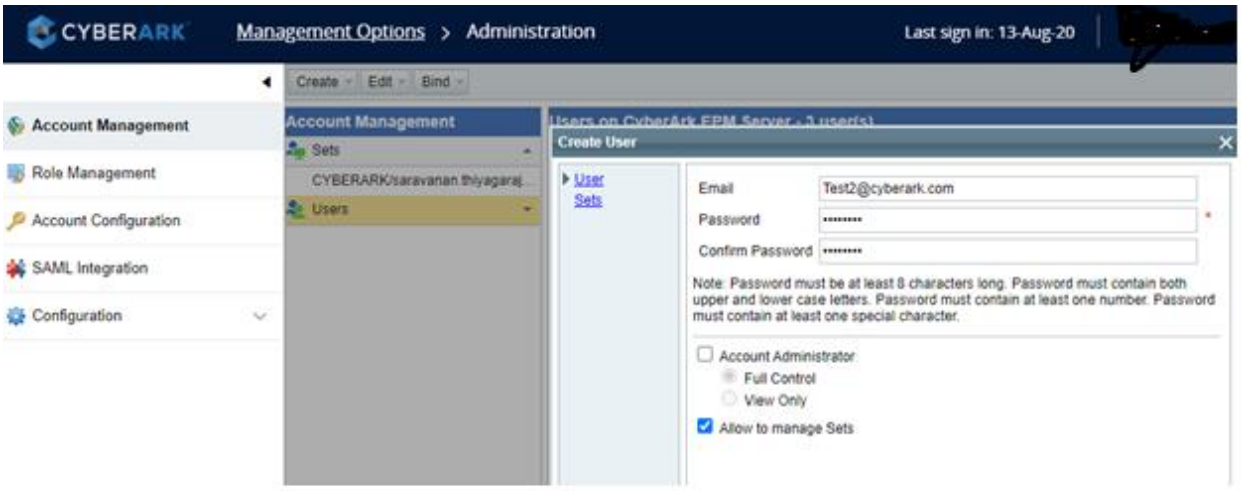
1.1 Login in to your EPM SaaS Admin Console as Administrator and Select Administration tab on the landing page. For example - Customers who had selected or chosen their Datacenter to be "US" will have received the link as "https://login.epm.cyberark.com/login" . The Admin Console Link may vary depending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



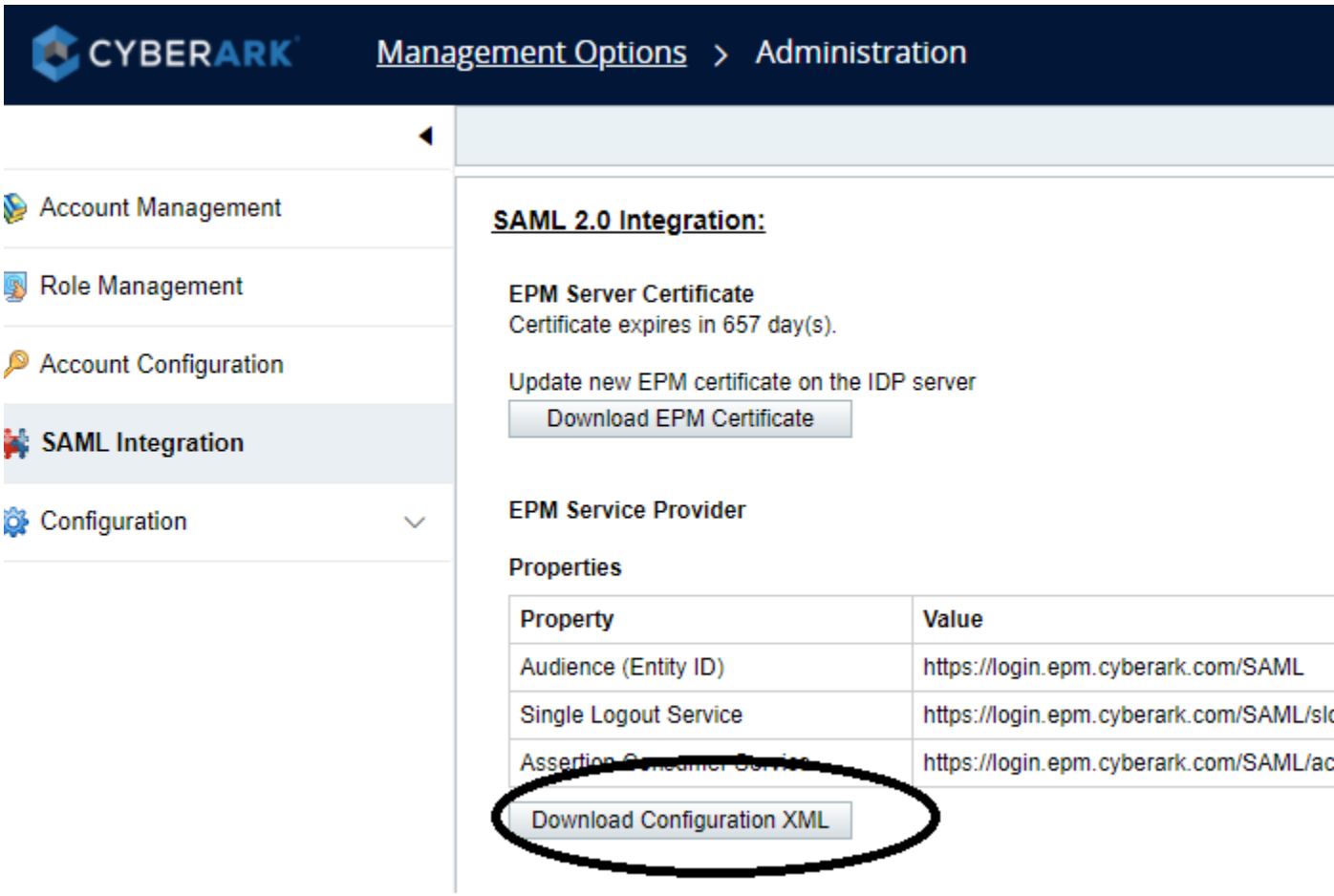

1.2 Select "Administration" tile and Under Account Management, please make sure to import/create other Administrators User Account (who will manage the EPM Policies) , View/Read only Accounts, leveraging email id and grant them require permission as "Account Administrator" or "Allow to manage sets".

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

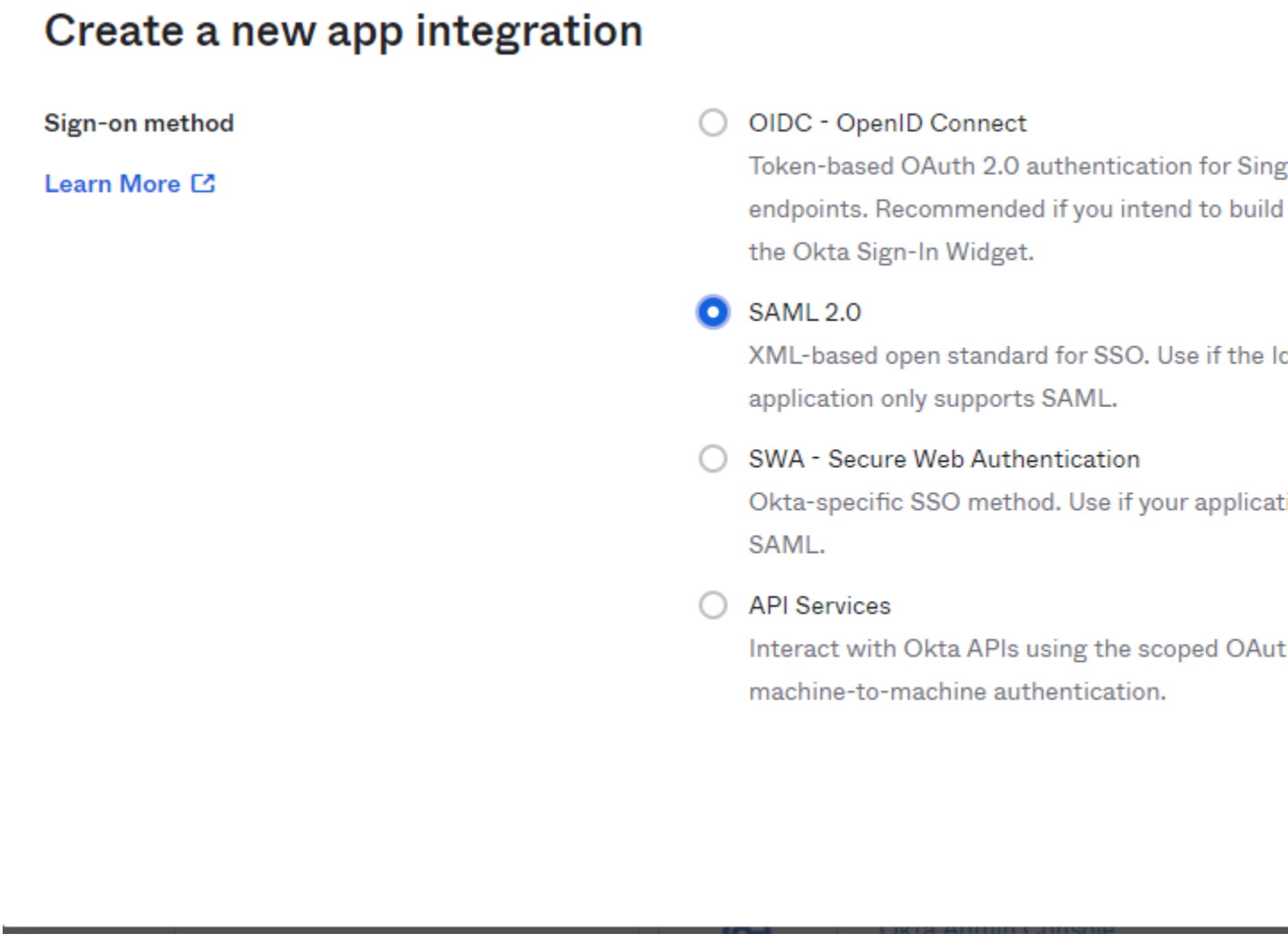



1.3 Please make sure to download the XML (metadata) file and Certificate from the EPM Admin Console. Logon to the EPM Administrative console as "Administrator" and select "Administration" Icon and Click on the SAML Integration. Under "**EPM Service Provider**" **please click "Download configuration XML"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



# 2: Configuration Steps in Okta to OnBoard CyberArk EPM SAML Application

2.1 Please logon to Okta Administrative Console and select “Create App Integration” and select “SAML2.0” in the next window and click Next.




2.2 Create SAML integration :

Under General Settings : Enter App name as “CyberArk Endpoint Privilege Manager” and click Next

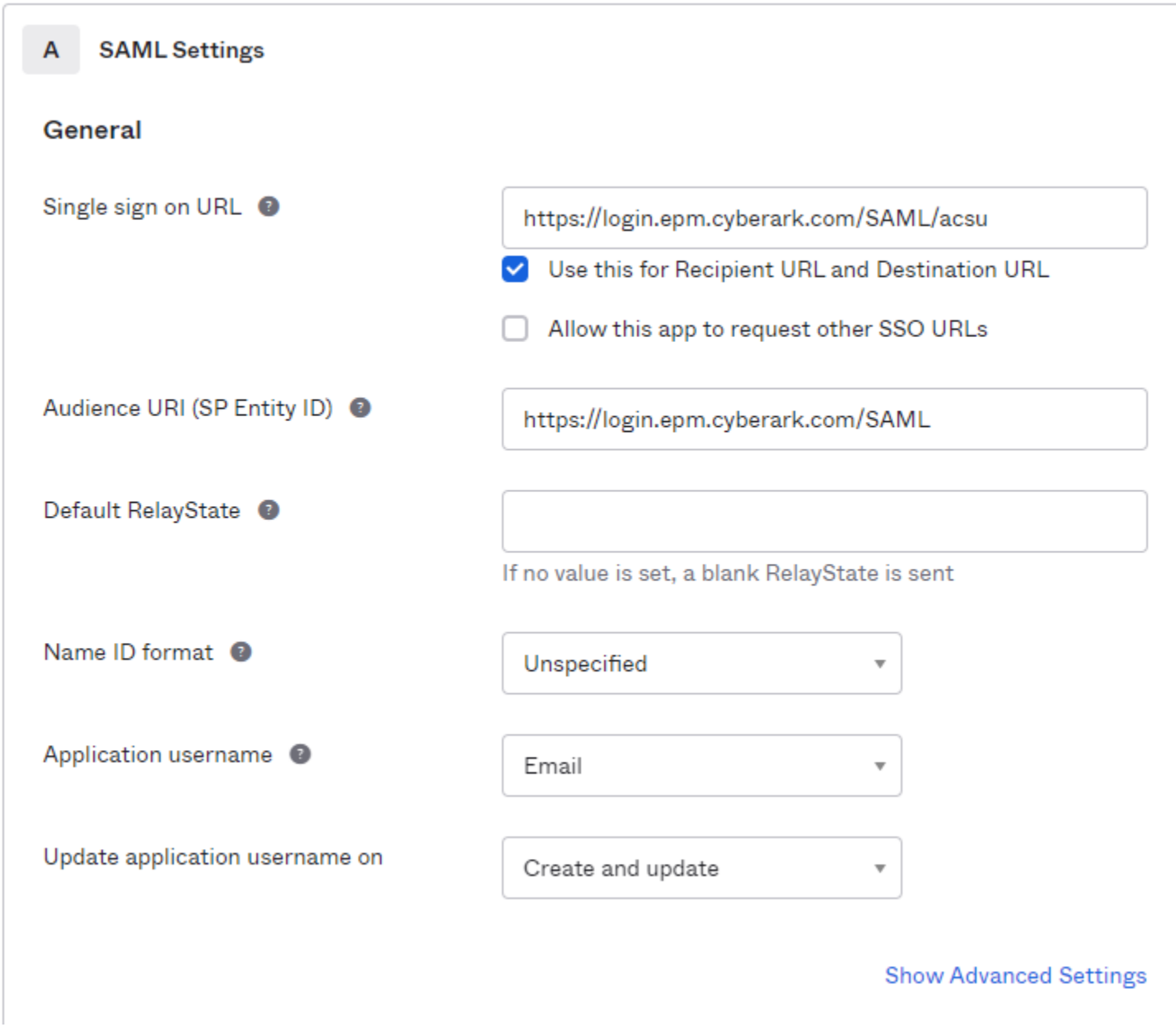
Under Configure SAML

Single Sign On URL : https://login.epm.cyberark.com/SAML/acsu

Audience URI (SP Entity ID) : https://login.epm.cyberark.com/SAML

Name ID Format: Unspecified

Application username:Email




Click Next

**2.3 : Help Okta Support understand how you configured this application**

Are you a customer or partner? Choose Customer and leave the rest to default.

Click Finish.

2.4 : On the Sign On page click “View Setup Instructions”,

# Cyberark End point Privilege Manager

Active ▾ View Logs Monitor Imports

General | Sign On | Mobile | Import | Assignments

## Settings

Edit

### Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

SAML 2.0

Default Relay State

**SAML 2.0** is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

### Credentials Details

| | |
|---|---|
| Application username format | Okta username |

Copy all the values to your local system and download the certificate.

Identity Provider Single Sign-On URL: https://dev-387858.oktapreview.com/app/dev-387858_cyberarkendpointprivilegemanager_1/exkzyx7qfhBHm5tLx0h7/sso/saml

Identity Provider Issuer: http://www.okta.com/exkzyx7qfhBHm5tLx0h7

X.509 Certificate: <Download the cert>

**2.5: Click Assignments:**

**Assign this application by adding a particular group or users.**

# 3.Configuration Steps in CyberArk EPM AdminConsole

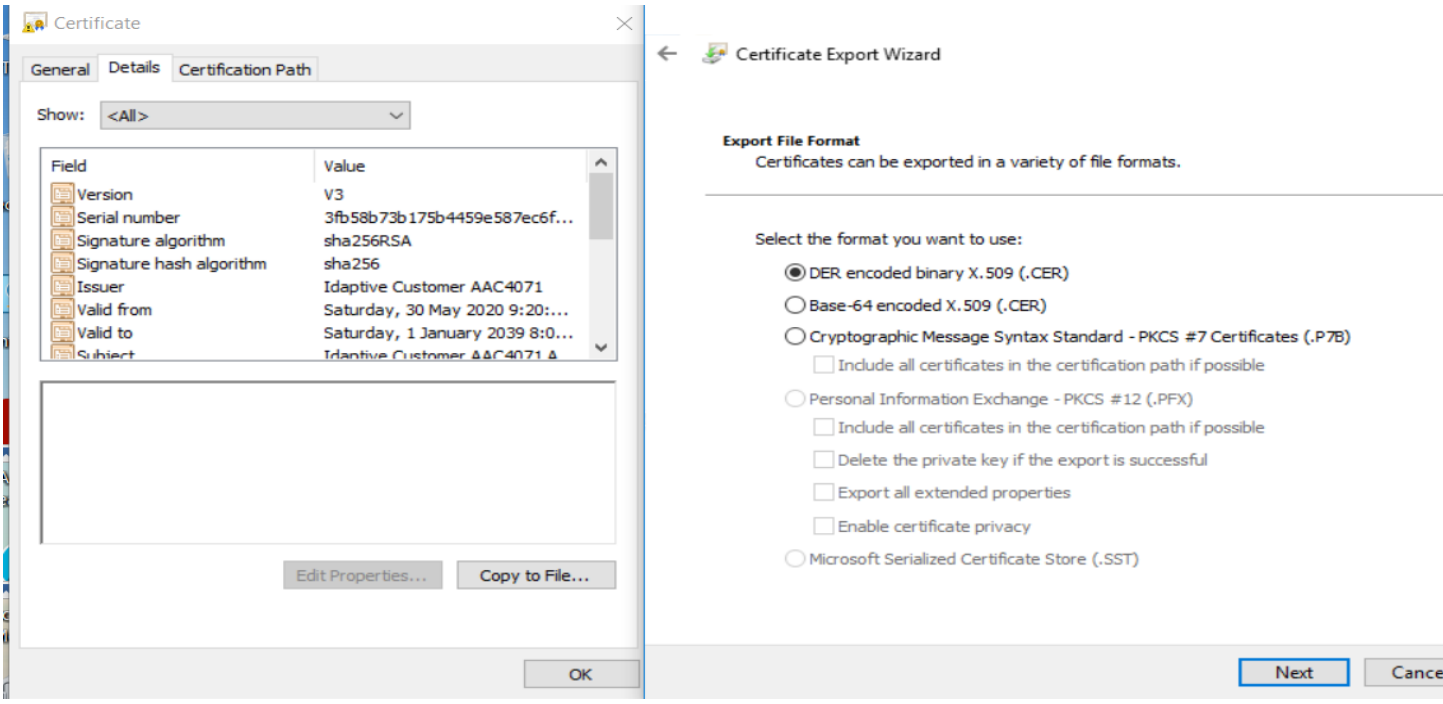
3.1 Login in to your EPM SaaS Admin Console as Administrator and select "Administration" tile and Choose "SAML Integration" and edit the configuration as follows.

Following values are required from Okta to complete the setup

| | |
|---|---|
| IDP Issuer URL | http://www.okta.com/exkzz1ae3cAKAdKFD0h7 |
| IDP Server Certificate | <Upload the certificate that you had downloaded from Okta > |
| IDP Single Sign On URL | https://dev-387858.oktapreview.com/app/dev-387858_cyberarkepm_1/exkzz1ae3cAKAdKFD0h7/sso/saml |
| 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. The value of idpid is important and can be obtained from Okta Admin Console.

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



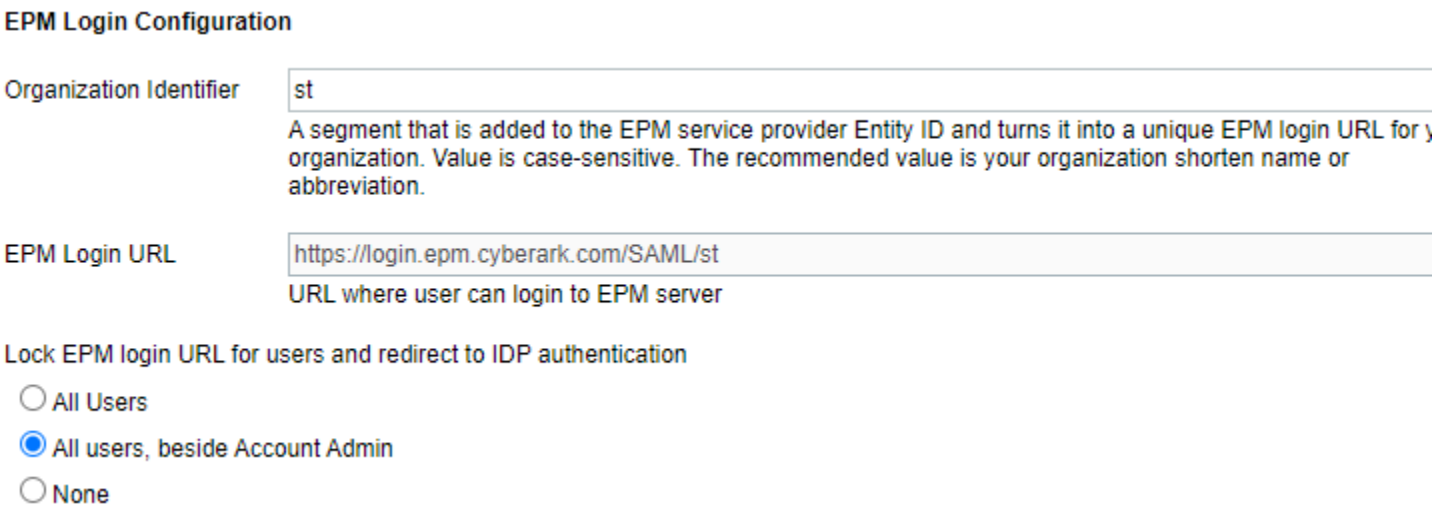

### 3.2 **EPM Login Configuration**

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>



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 Okta.
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.