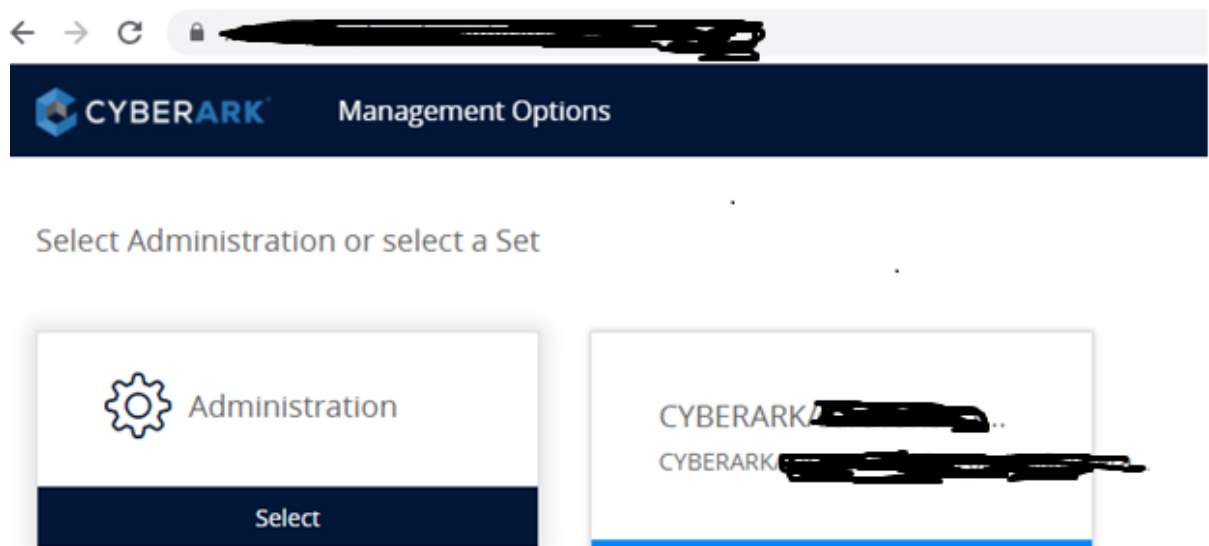


Enabling SAML Integration with Microsoft ADFS for EPM SaaS

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.

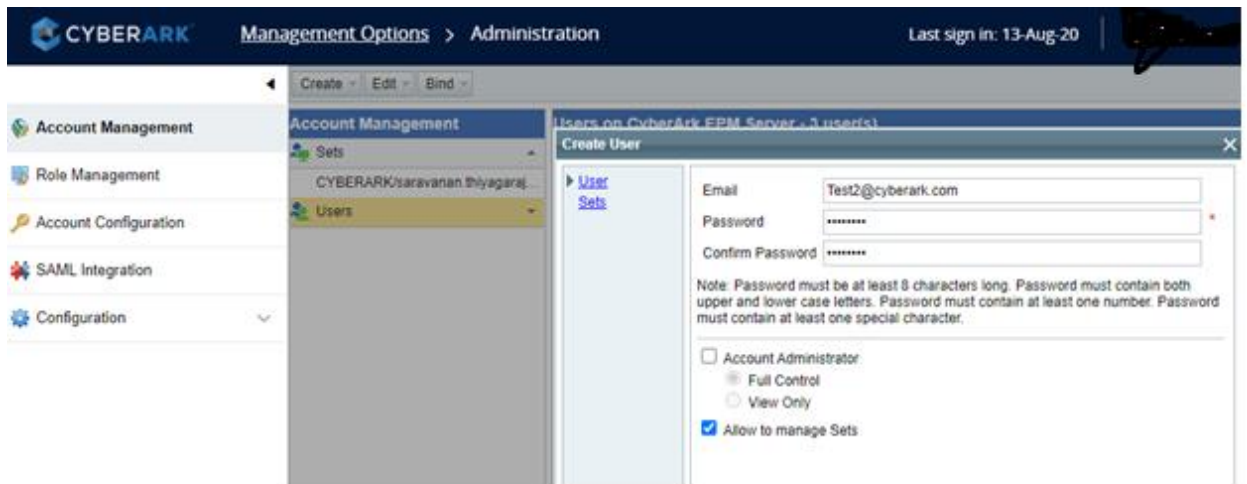


- 1.2 Select "Administration" tile and Under Account Management, please make sure to import/create other Administrators User Account (who will manage the EPM Policies) , View/Read only Accounts, leveraging email id and grant them require permission as "Account Administrator" or "Allow to manage sets".

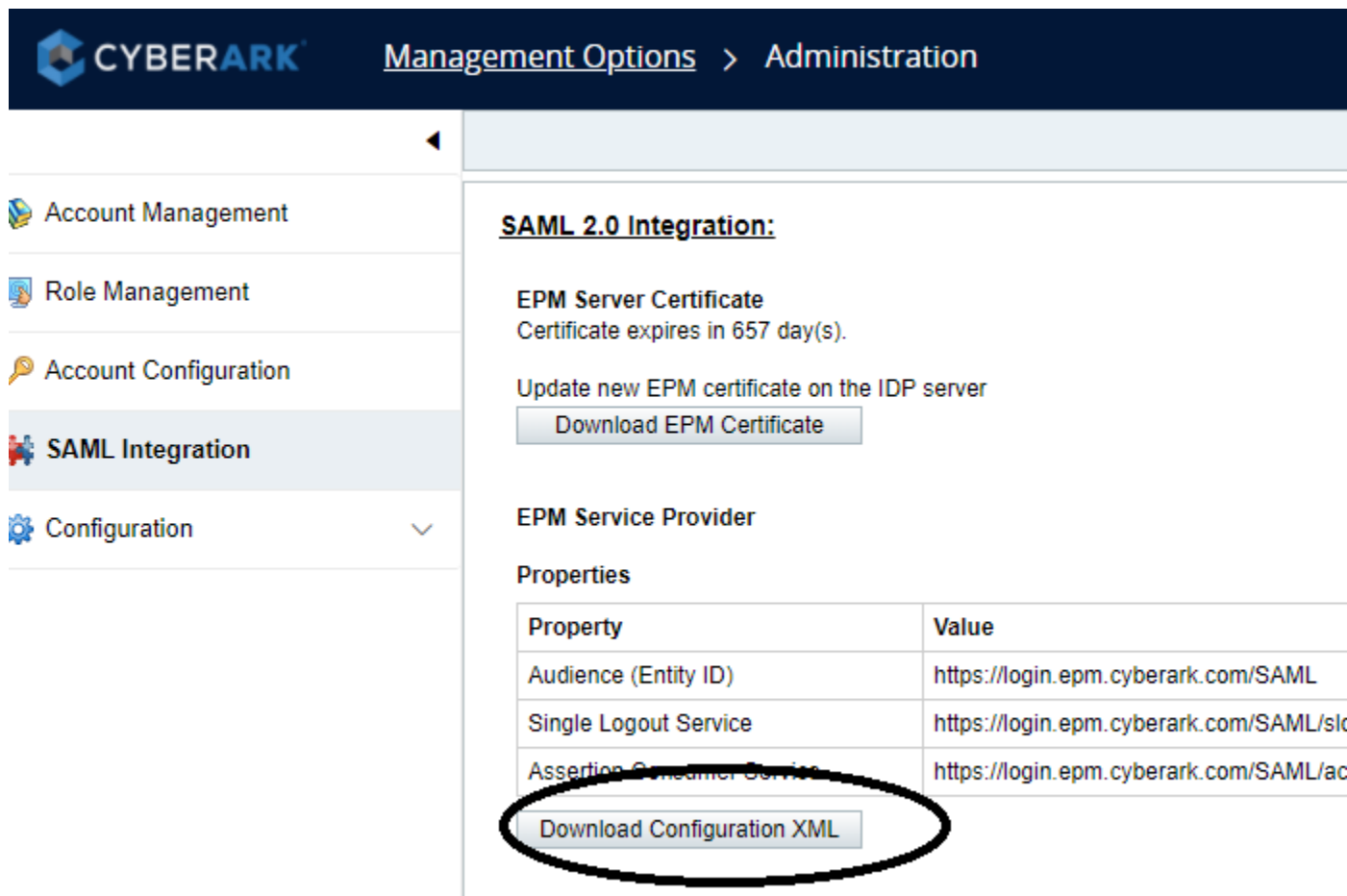
The accounts that are created in EPM, will get authenticated thru Single Sign on and MFA .

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 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 ADFS Server.



2: Pre-requisites on Microsoft ADFS

Please make sure the ADFS is installed and configured correctly. You can test your ADFS Environment by accessing the below link.

Opening a web browser and navigating to the following url

<https://<ADFS FQDN>/adfs/ls/IdpInitiatedSignon.aspx>. You will be prompted to enter your AD credentials once you have supplied your credentials and successfully logged on you will see the following page indicating you have been successfully logged in.

Please make sure the Users exist in your Active Directory.

Sign-In Page

You are signed in.

Sign Out

Sign out from all the sites that you have accessed.

Sign Out

Sign out from this site.

2: Configuration Steps in ADFS to onboard EPM Application

2.1 Please login to ADFS Server and launch Server Manager. Go to Tools Menu and click AD FS Management. We need to configure EPM Admin App as “Relying Party Trusts” in ADFS

AD FS

File Action View Window Help

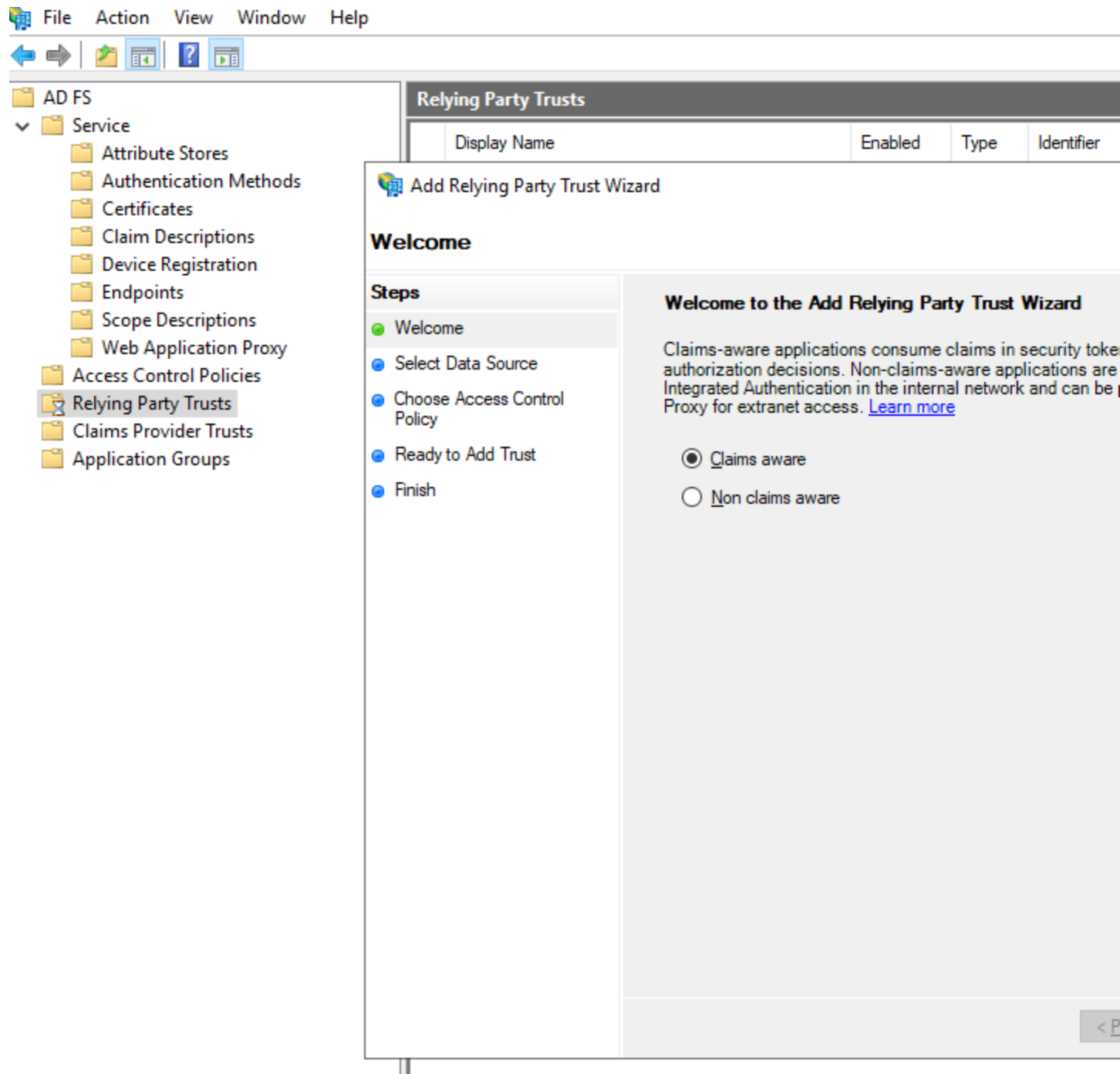
AD FS

- Service
 - Attribute Stores
 - Authentication Methods
 - Certificates
 - Claim Descriptions
 - Device Registration
 - Endpoints
 - Scope Descriptions
 - Web Application Proxy
- Access Control Policies
- Relying Party Trusts**
- Claims Provider Trusts
- Application Groups

Relying Party Trusts

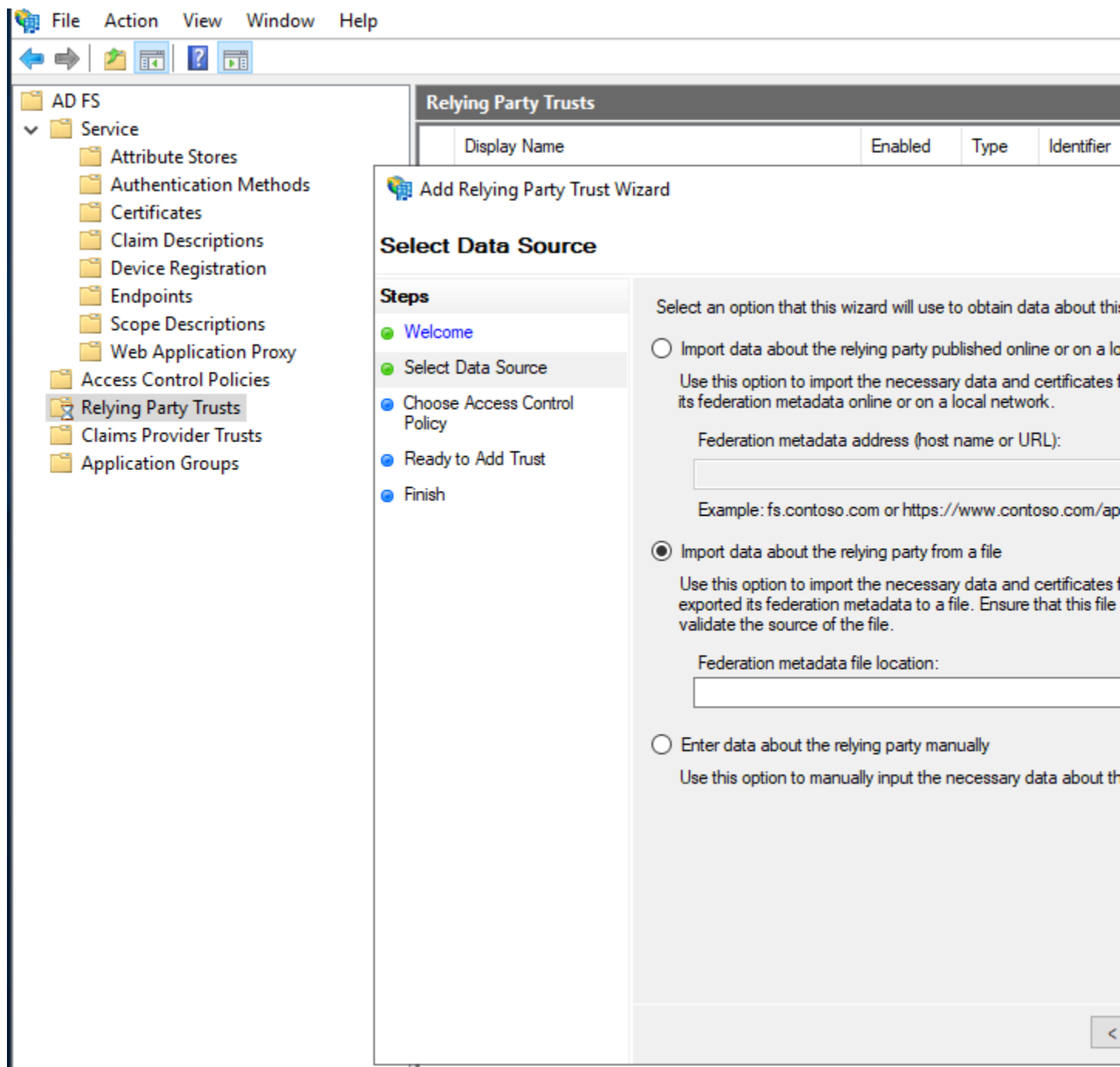
Display Name	Enabled	Type	Identifier
EPMAAdminConsole	Yes	WS-T...	https://log

2.2 Click “Relying Party Trust” and click “Add Relying Party Trust”. Choose “Claims aware” and click start.



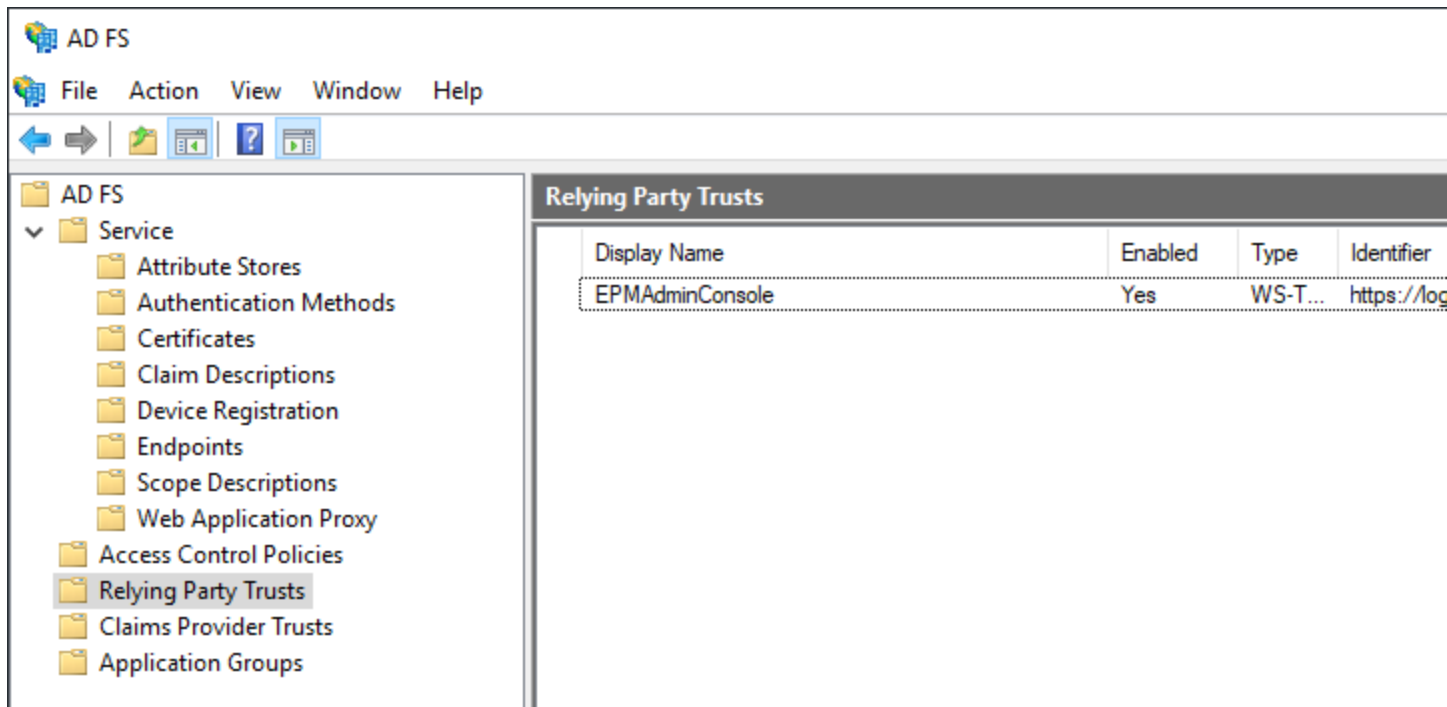
2.3 Select the Option to “Import data about the relying Party from a file” or Manually “Enter data about the relying Party”. This guide reference to “Import data about the relying party”. Browse and upload the xml file and click next.

XML file details are described in section 1.3.



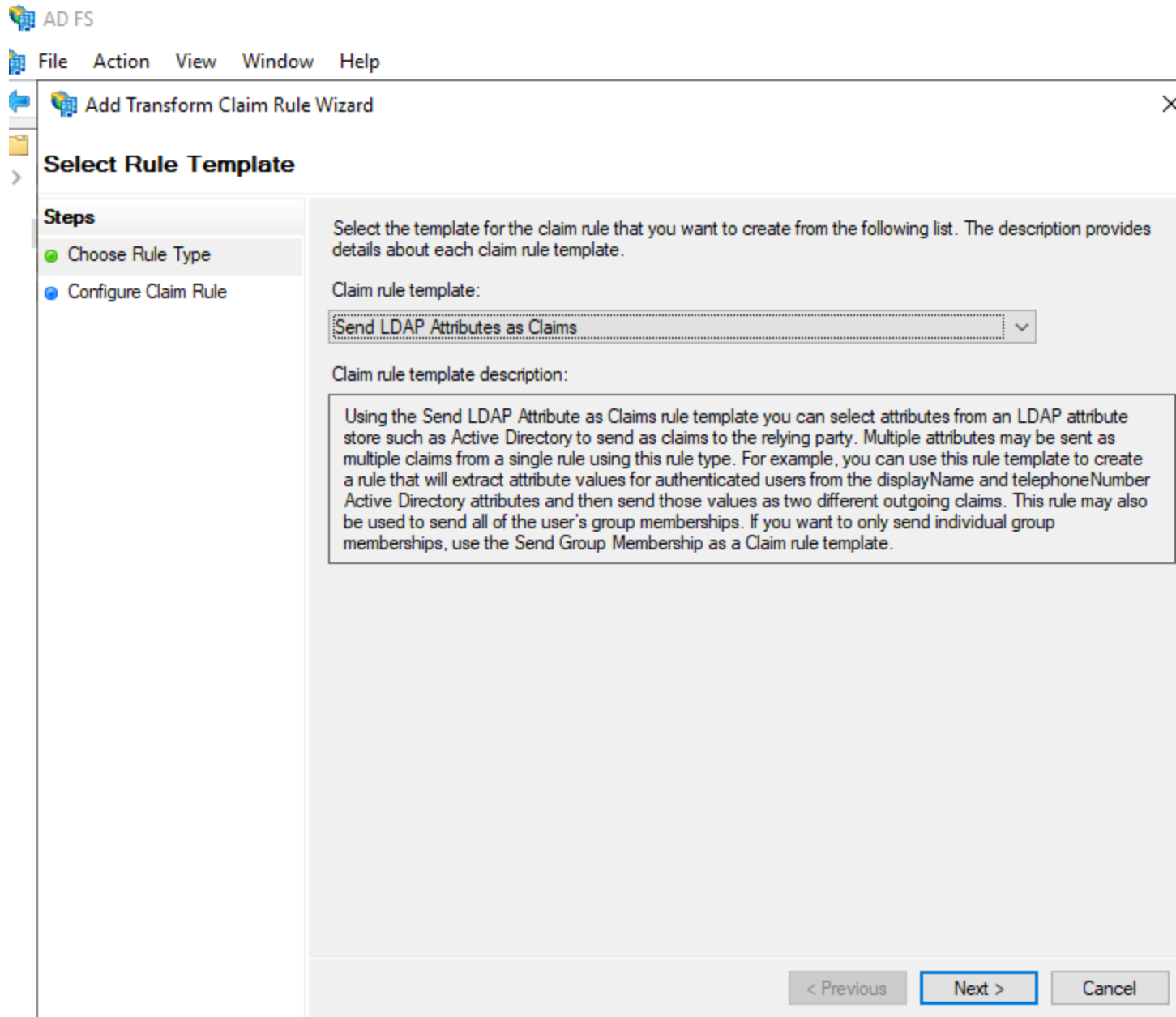
2.4 Provide Display name as your interest .For example – EPM Admin Console and click next. Choose “Permit everyone” under Access Control policy and click Next and finish.

Note – “Choose an Control Access policy” is customizable and choose your best choice.



2.5 Configuring the “Claim Issuance Policy” for the EPM AdminConsole

Select the Display Name -> click “Edit Claim Issuance Policy” -> click “Add Rules”.



2.6 Click Next and provide a Claim Name, select the Attribute Store as “Active Directory” and from the Dropdown select the attributes and map them as shown below and click ok.

Edit Rule - GetLdapAttributes

×

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

GetLdapAttributes

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
	Given-Name	Given Name
	SAM-Account-Name	Common Name
*		

View Rule Language...

OK

Cancel

2.7 Add another claim rule as below. Choose “Transform an Incoming Claim” and click next.

 Add Transform Claim Rule Wizard

×

Steps

● Choose Rule Type

● Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

▼

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

< Previous

Next >

Cancel

2.8 Provide a claim rule name and select and configure the attributes as shown below and click Finish.

 Add Transform Claim Rule Wizard✕

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

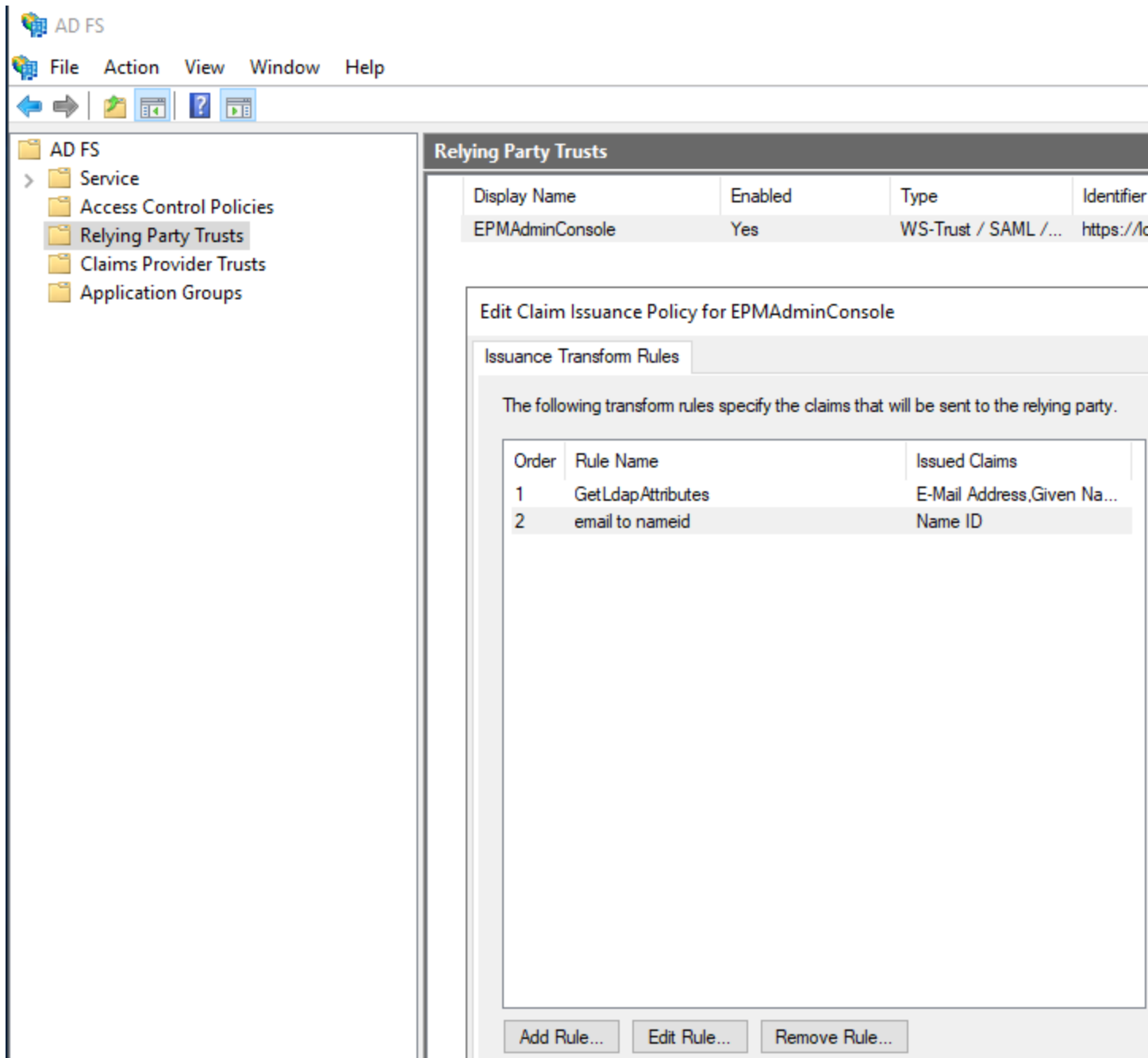
Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

2.9 After finishing the above steps, you should see similar configuration on your screen. (Just as an reference)



2.10– Export the Certificate from ADFS and store them locally.

Expand the Service and click Certificates under ADFS and click on the Toekn-Signing and click “copy to file” and save the certificate locally. When you export the certificate please make sure to choose “Der encoded binary” X.509 (.cer)/

AD FS

File Action View Window Help



AD FS

Service

Attribute Stores

Authentication Methods

Certificates

Claim Descriptions

Device Registration

Endpoints

Scope Descriptions

Web Application Proxy

Access Control Policies

Relying Party Trusts

Claims Provider Trusts

Application Groups

Certificates

Subject	Issuer	Effective Date	Expiration Date
Service communications			
CN=DC.bdlab01.com	CN=DC.bdlab01.com	9/10/2020	9/10/2021
Token-decrypting			
CN=ADFS Encryption - DC...	CN=ADFS Encryption - D...	9/10/2020	9/10/2021
Token-signing			
CN=ADFS Signing - DC.bdl...	CN=ADFS Signing - DC.b...	9/10/2020	9/10/2021

Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	1aeece1685ce1d8aa4f3528004...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - DC.bdlab01.com
Valid from	Thursday, September 10, 202...
Valid to	Friday, September 10, 2021 9...
Subject	ADFS Signing - DC.bdlab01.com

Edit Properties... Copy to File...

OK

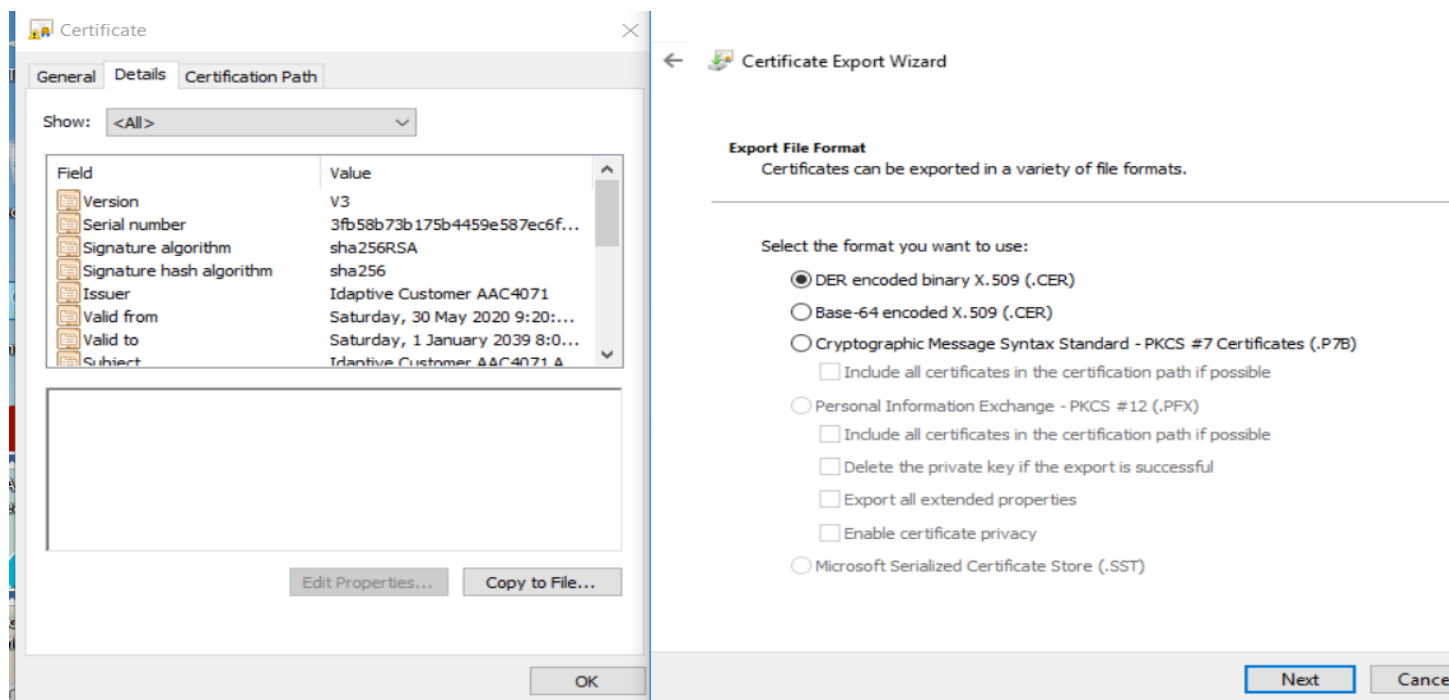
3.Configuration Steps in CyberArk EPM AdminConsole

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 ADFS to complete the setup

IDP Issuer URL	http://< ADFS FQDN > /adfs/services/trust
IDP Server Certificate	<Upload the certificate from ADFS>
IDP Single Sign On UR	https://< ADFS FQDN > /adfs/ls
IDP Single Logout URL	https://< ADFS FQDN > <ADFS Custom logout end point>

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/wsederation?wa=wsignout1.0>>

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 ADFS

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

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