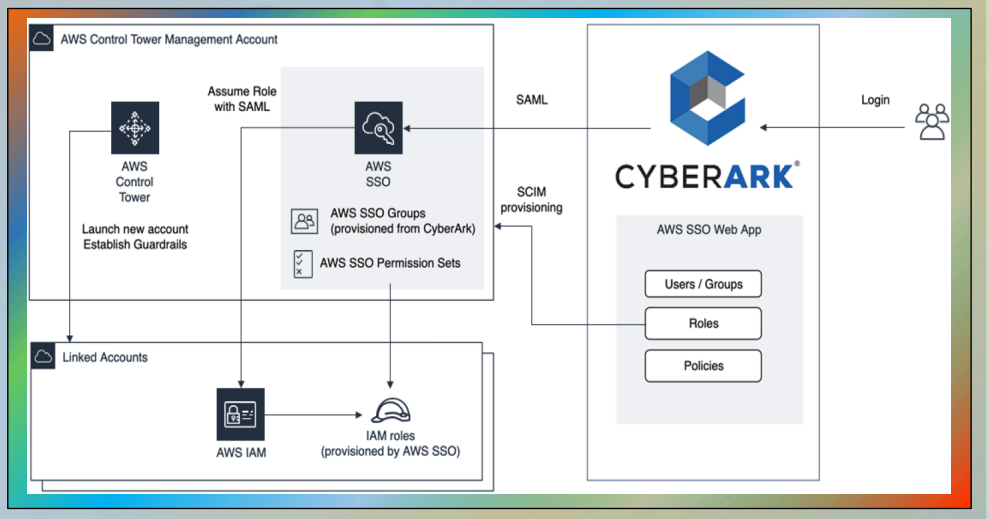
https://linkedin.com/in/praful patel16

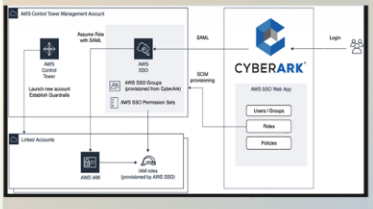
https://github.com/praful patel16

AWS PROJECT

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH CYBERARK WORKFORCE IDENTITY

IMPLETENTED BY: PRAFUL PATEL





Date: June 08, 2022

- **Project Definition:**

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH CYBERARK WORKFORCE IDENTITY

- **Project Description:**

An IT services Provider Company **PRAfect Systems Inc.** is engaged into providing Cloud/DevOps & software development solutions. Recently, the company had to run into IAM identity access and management issues due to their huge workload and multiple integrations of the third party application accessibility. The company has decided to move take a benefit of third party IAM service provider "CyberArk" in order to manage the entire user management at one central place.

Management has decided to enable a Single Sign-On feature within AWS and integrate that with the 'cyberark" external workforce identity provider and come up with small POC project which can prove the entire integration and insights into the AWS SSO feature.

This project demonstrates an experience of deploying and integrating "Cyberark" external third party Identity provider and web identity federation using using AWS SSO.

- **Solution:**

AWS Single Sign-On (AWS SSO) is where you create or connect your workforce identities in Amazon Web Services (AWS) once and manage access centrally across your AWS Organization.

We recently announced a new integration with CyberArk Workforce Identity to provide simplified access management and provisioning to AWS.

As a supported identity provider (IdP) for AWS SSO, CyberArk Workforce Identity enables you to manage AWS user identities outside of AWS and give these users permissions to access AWS resources across all of your AWS Organizations accounts.

With this integration, you can have a single point of truth for all enterprise identities and enforce consistent management of users, groups, permissions, and access policies while reducing redundancies and errors.

AWS SSO allows customers to efficiently manage user identities at scale by establishing a single identity and access strategy across their own applications, third-party applications (SaaS), and AWS environments.

Benefits of using CyberArk Workforce Identity as an external IdP for AWS SSO are:

1. Centralized management of your enterprise and AWS identities to ensure consistent configuration, control, and reduction of errors across systems. With this integration, you don't need to manually create and maintain user identities in AWS Identity and Access Management (IAM).
2. Improved user experience with federated access to AWS accounts using Security Assertion Markup Language (SAML). Once set up, users can access different roles in AWS accounts with just two clicks without re authentication.
3. Streamlined provisioning using System for Cross-domain Identity Management (SCIM); once connectivity is established, changes to user attributes are automatically synched and access to AWS accounts can be added or removed as users change roles.
4. Leveraging Attribute-Based Access Control (ABAC) to provide granular access control to resources based on session tags.

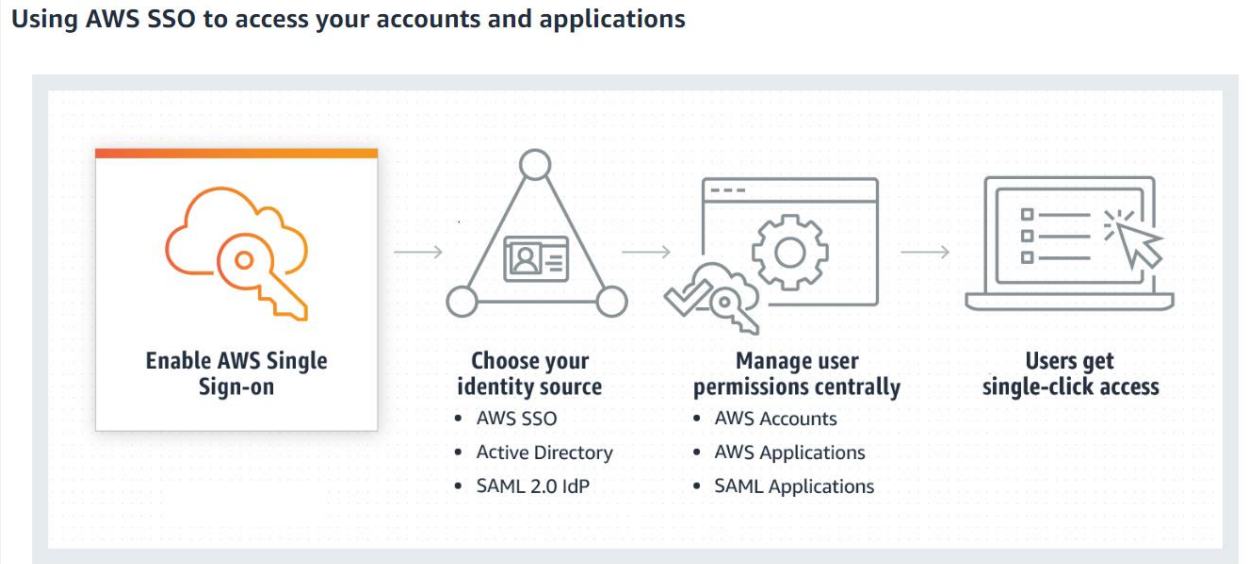
- **Project Cost Estimation:**

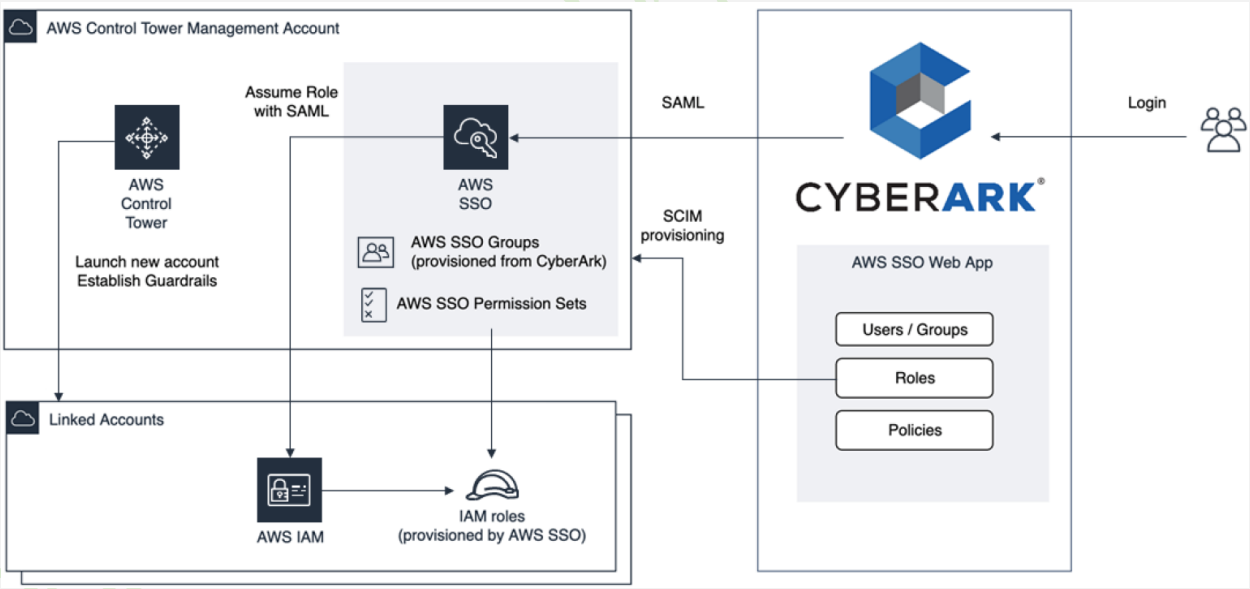
(Note: This cost is Not any actual cost, it's just an estimation based on high level requirement. Price may be vary based on adding and removing services based on requirement.)

- **Pre-requisites:**
  1. AWS SSO enabled- AWS Organization account
  2. CyberArk Workforce Identity on AWS Marketplace OR
  3. CyberArk Identity free trial sign-up

- **Tools & Technologies covered:**
  - AWS Single Sign-On(SSO)
  - CyberArk Identity provider
  - SAML 2.0 Authentication

➢ Solution Architecture:





➢ Implementation:

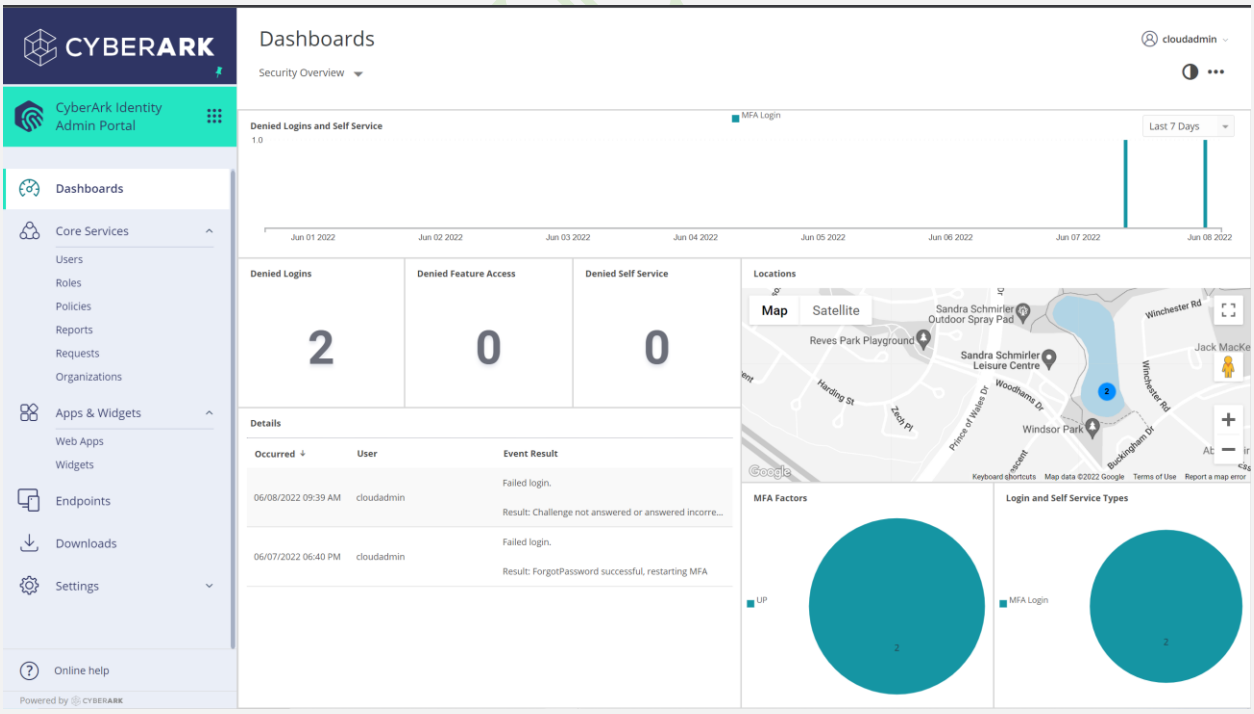
The steps we'll take are:

Setting up CyberArk Workforce Identity application with AWS SSO.
Configuring AWS SSO to use CyberArk Workforce Identity as an identity source using SAML.
Setting up SCIM between AWS SSO and CyberArk Workforce Identity.

- **Implementation in an Action:**

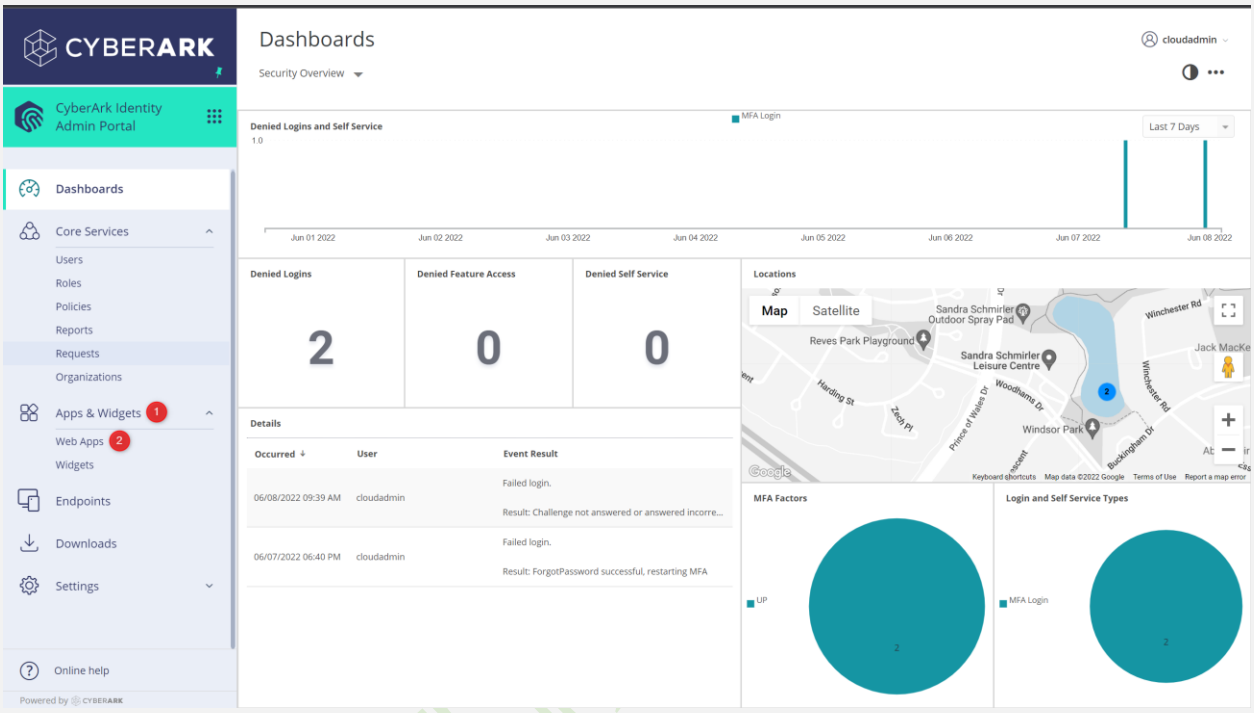
Login to Admin Portal

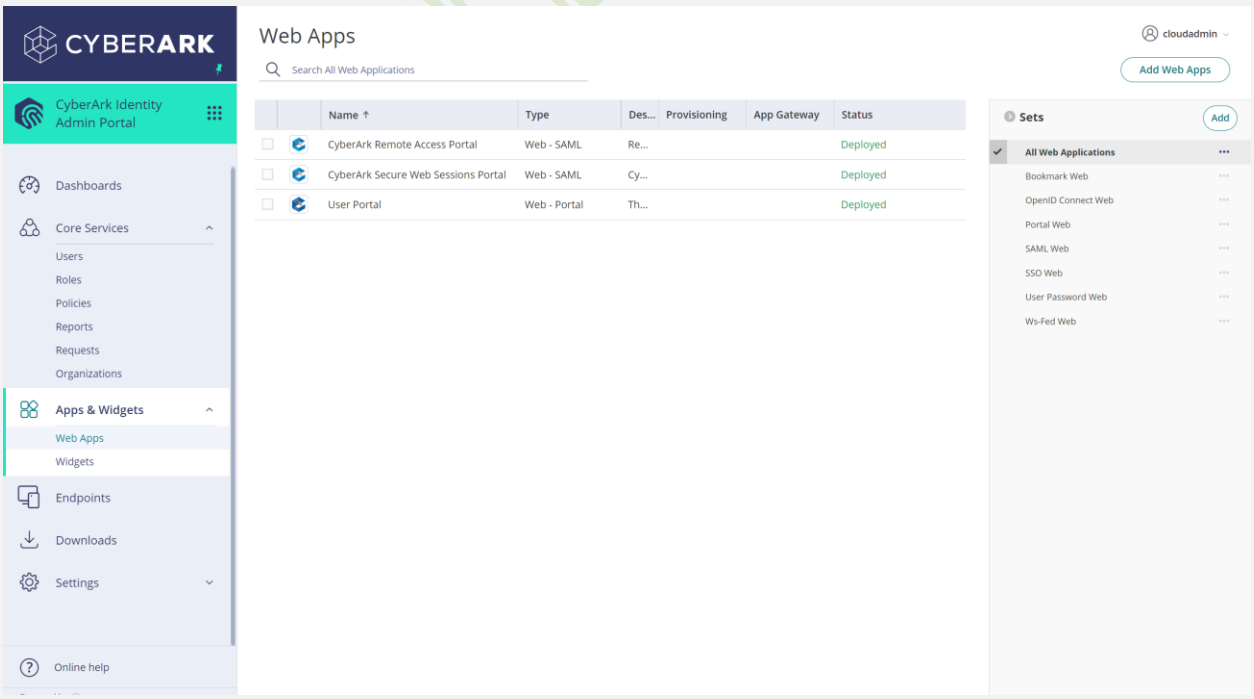
Dashboard

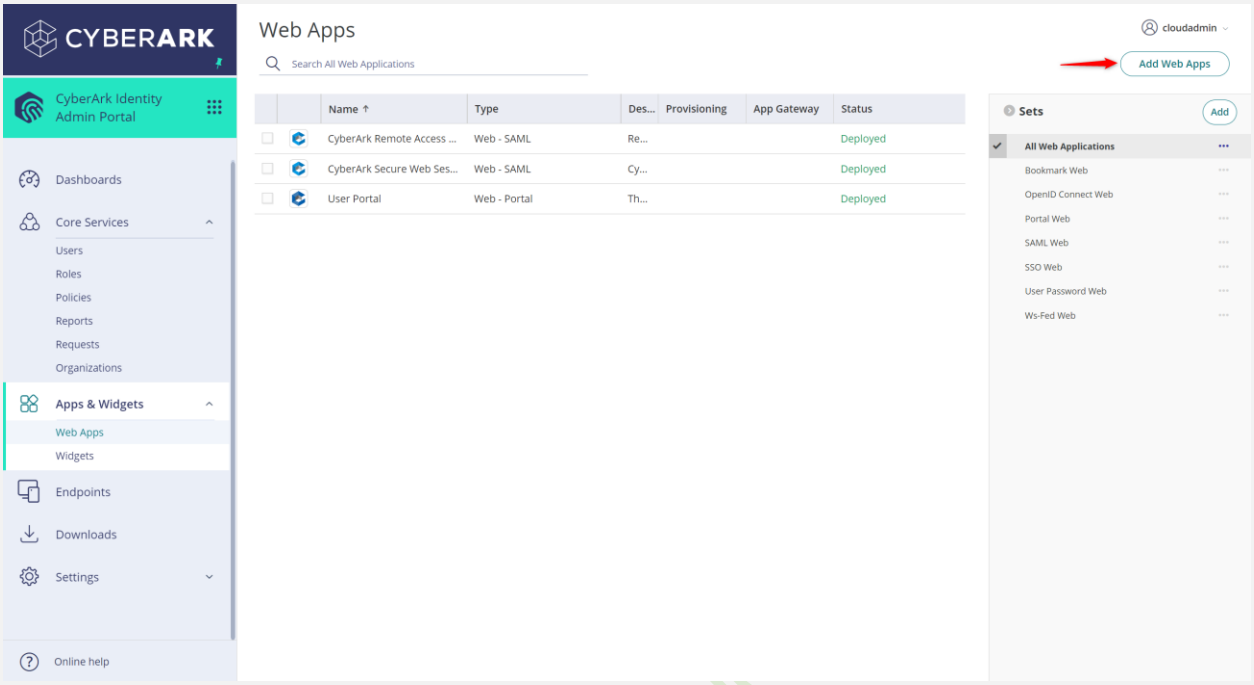


1. Sign in to the CyberArk Workforce Identity admin portal.
2. Choose Apps, Web Apps.

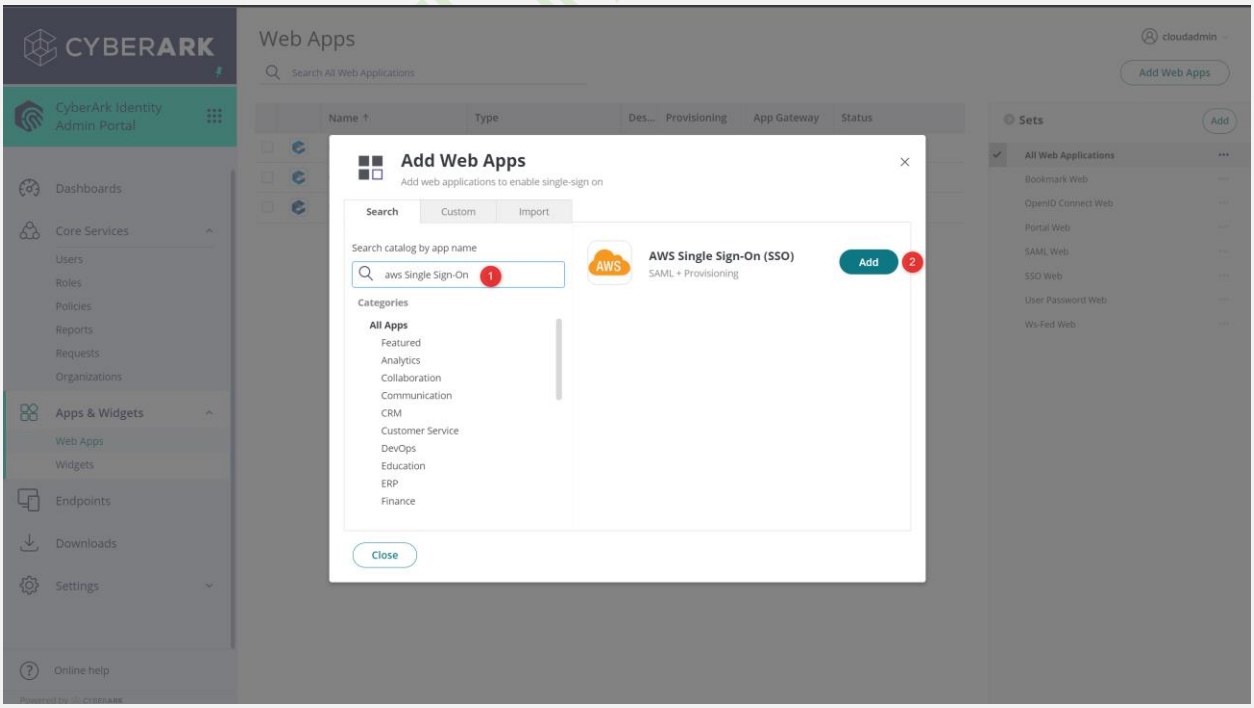
3. Choose Add Web App.
4. Search for AWS Single Sign-On, and choose Add.

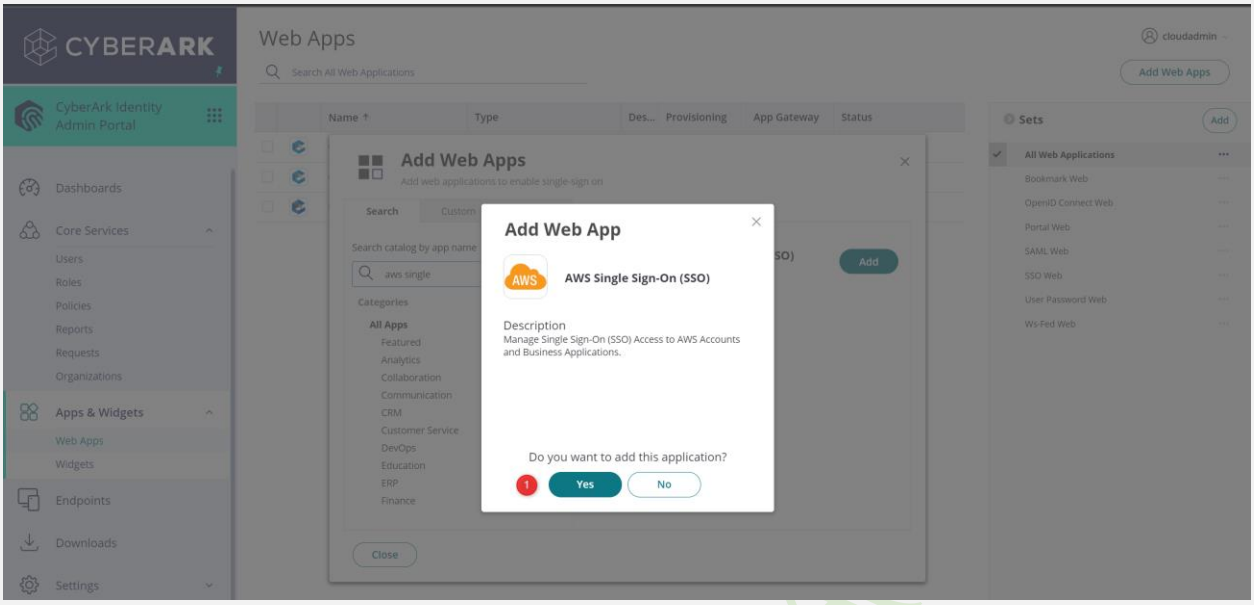




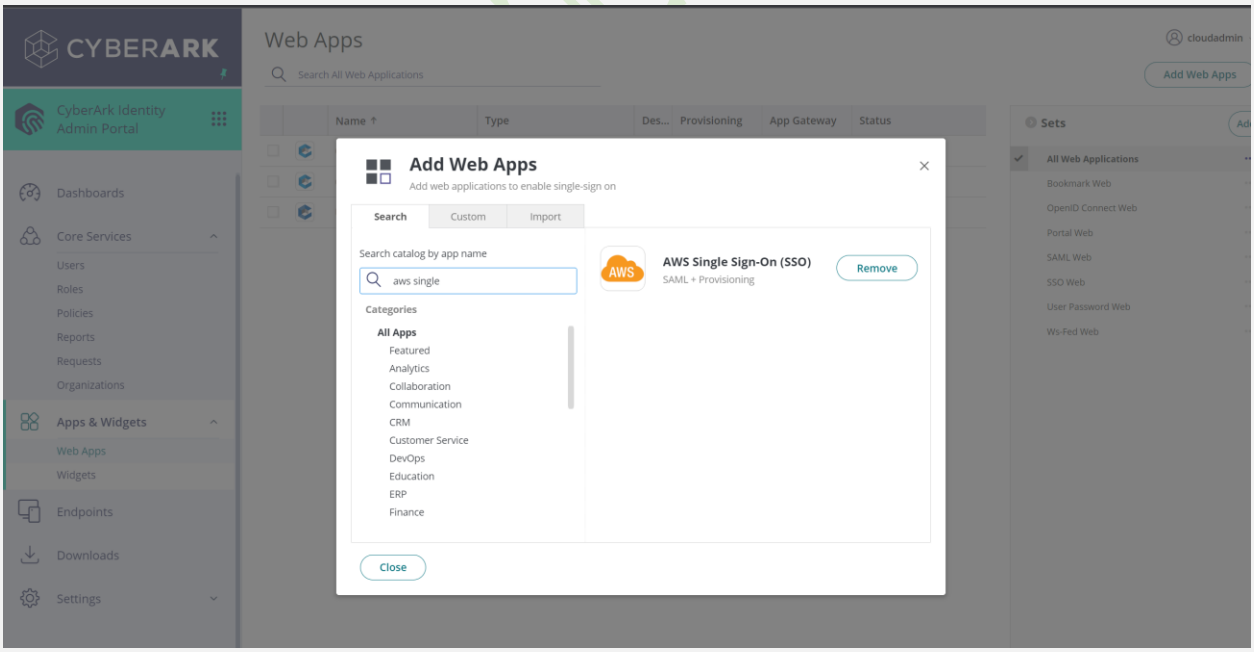


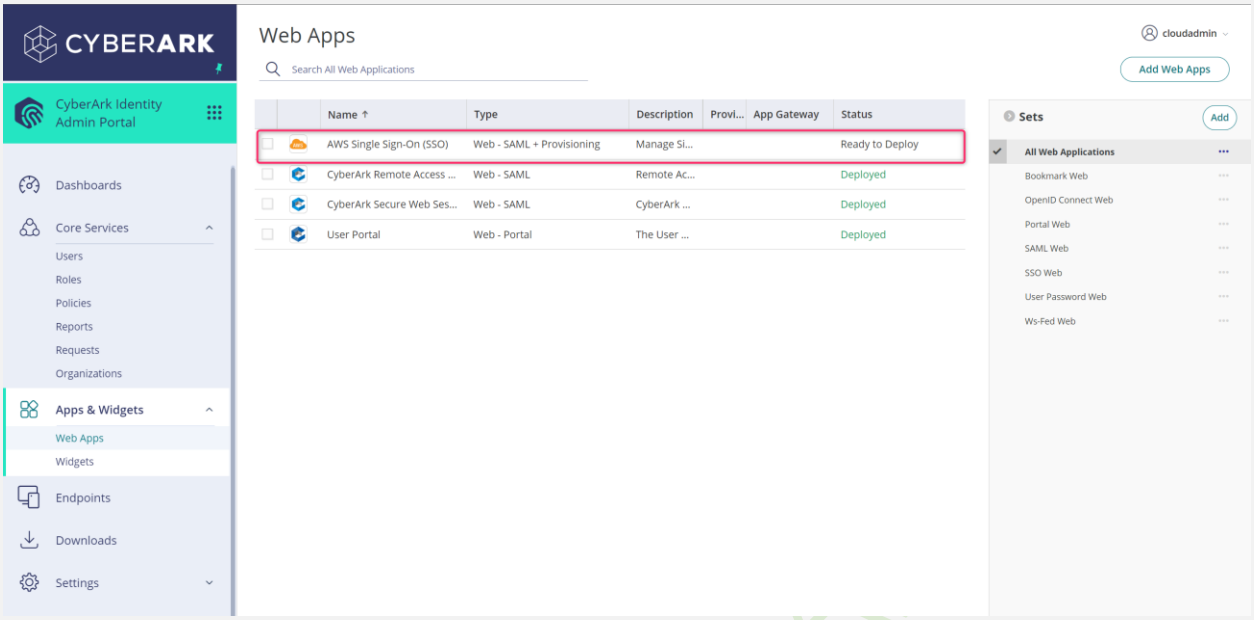
Search for AWS Single Sign-On, and choose Add.

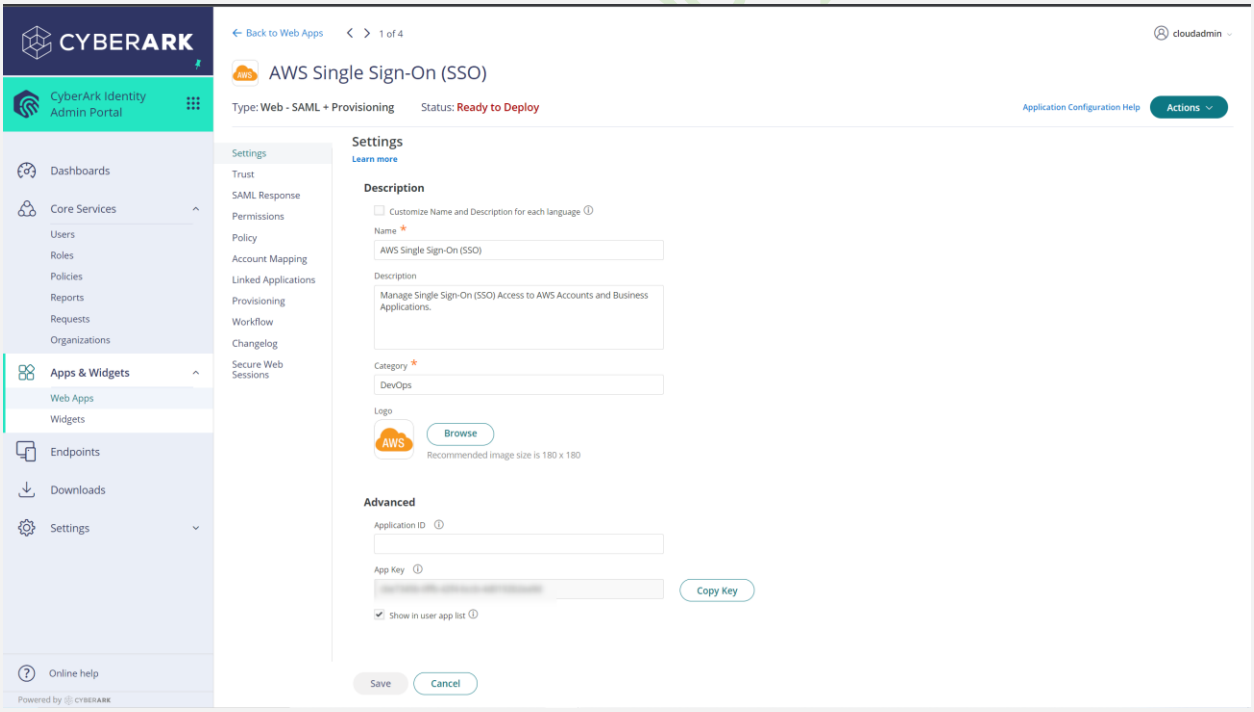




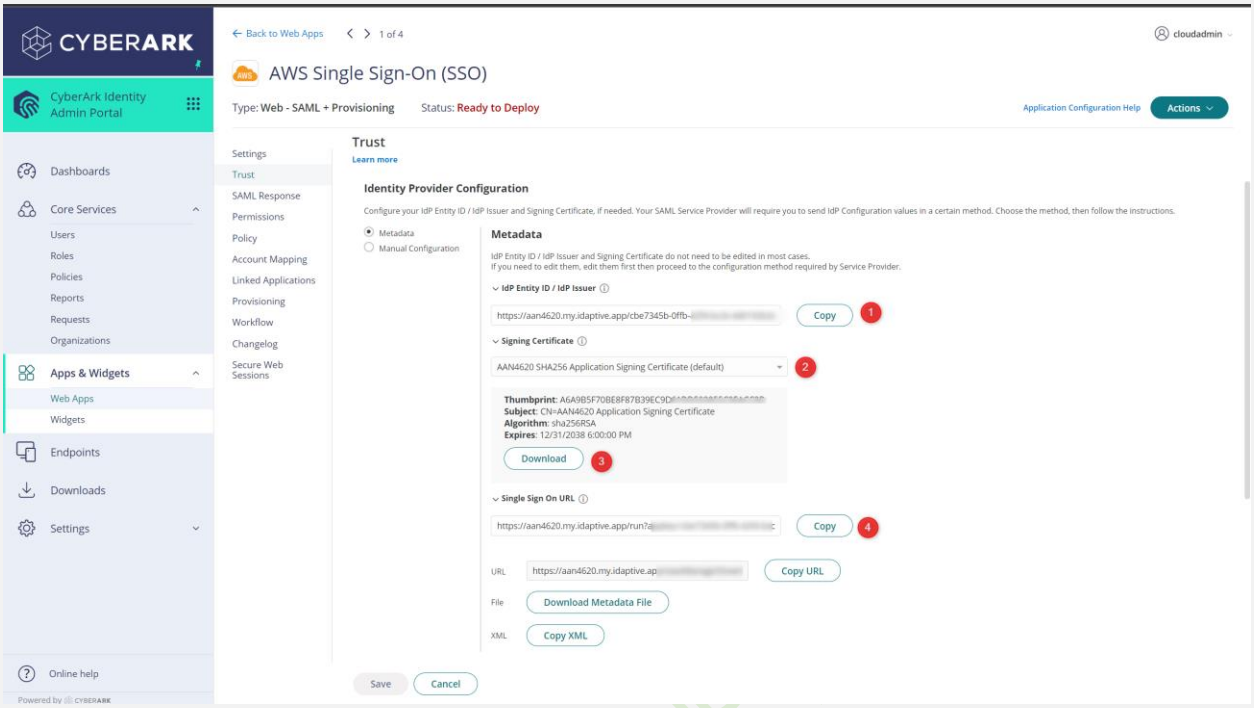
5. In the AWS SSO application you just created, go to Trust to set up SAML.
6. At the top, under Identity Provider Configuration, copy the IdP Entity ID and Single Sign-On URL to be used later to set up AWS SSO.
7. Download the Certificate to be used later in AWS SSO.



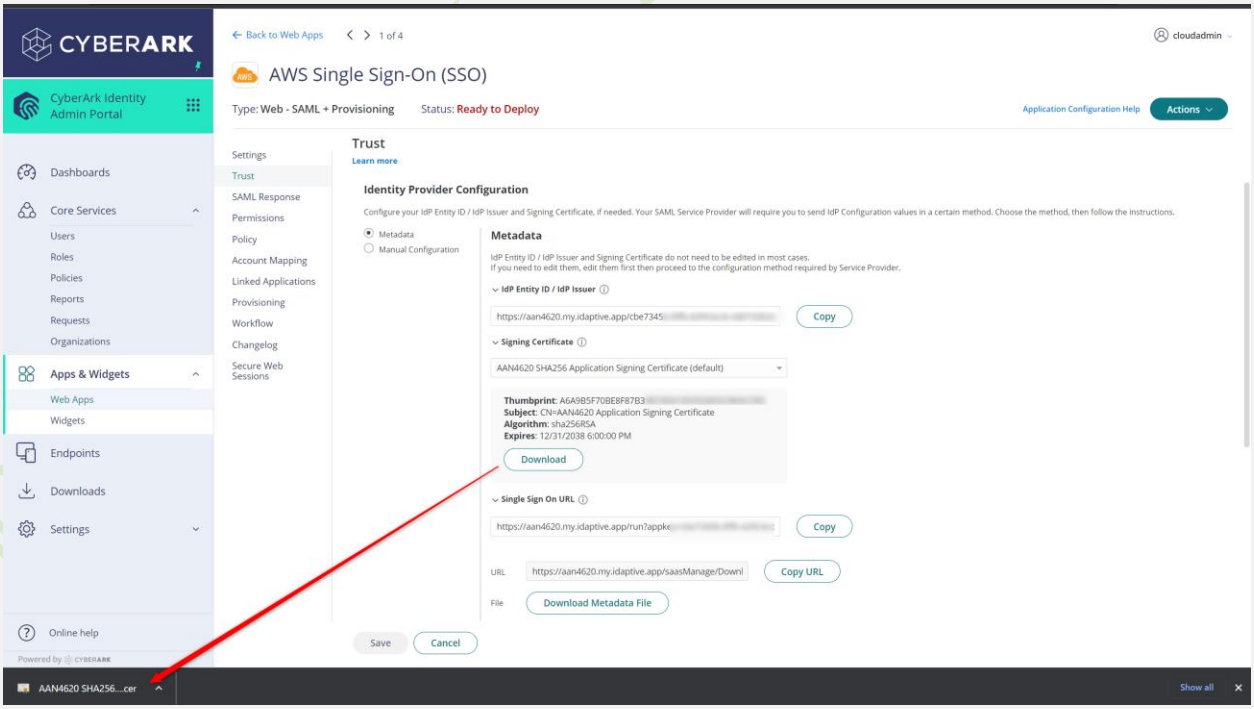




5. At the top, under Identity Provider Configuration, copy the IdP Entity ID and Single Sign-On URL to be used later to set up AWS SSO.

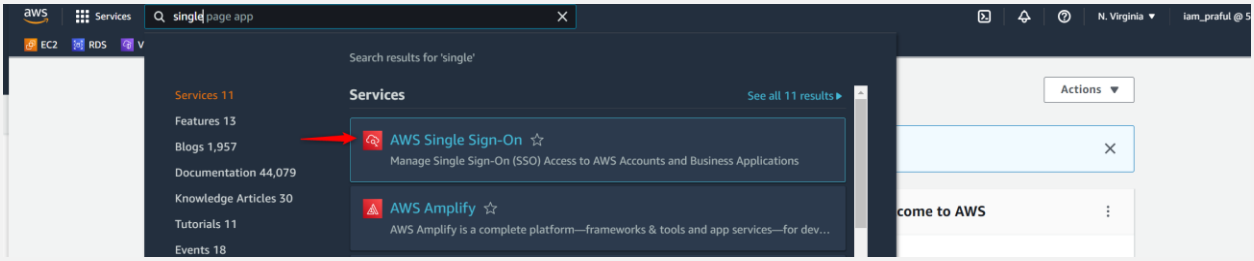


5. Download the Certificate to be used later in AWS SSO.

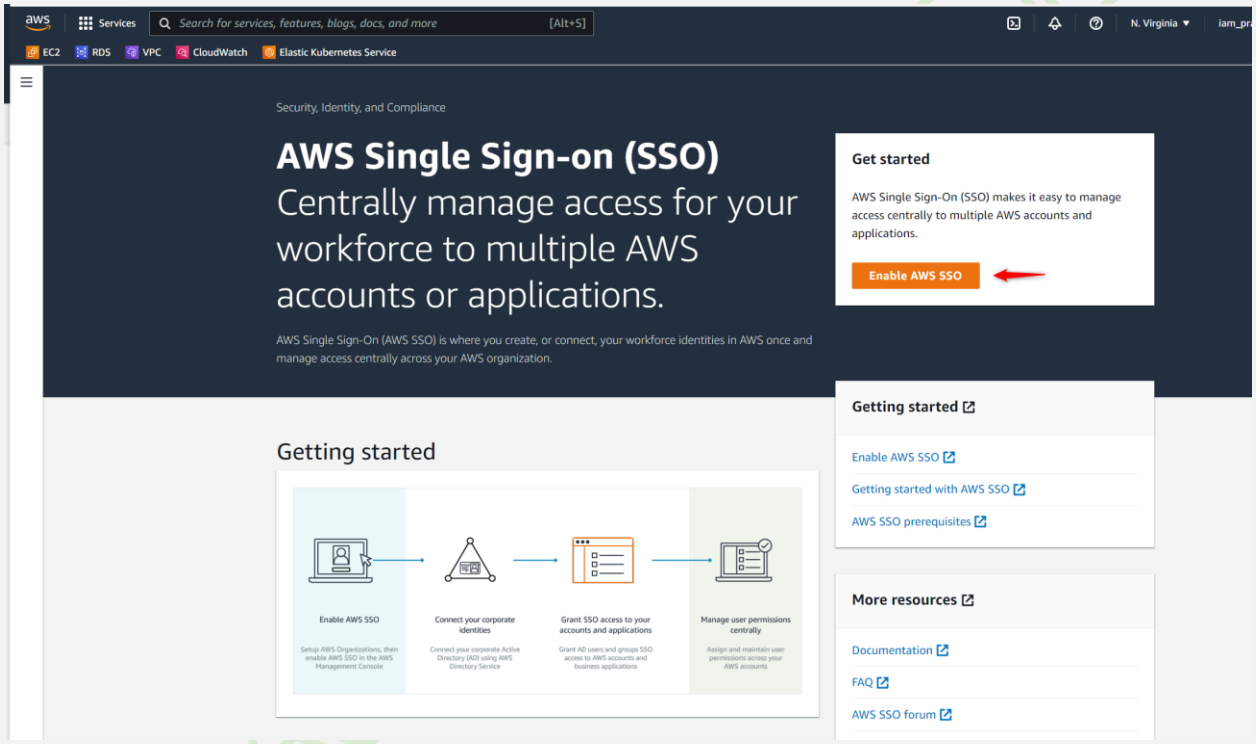


6.
7. Configuring New External Identity Provider

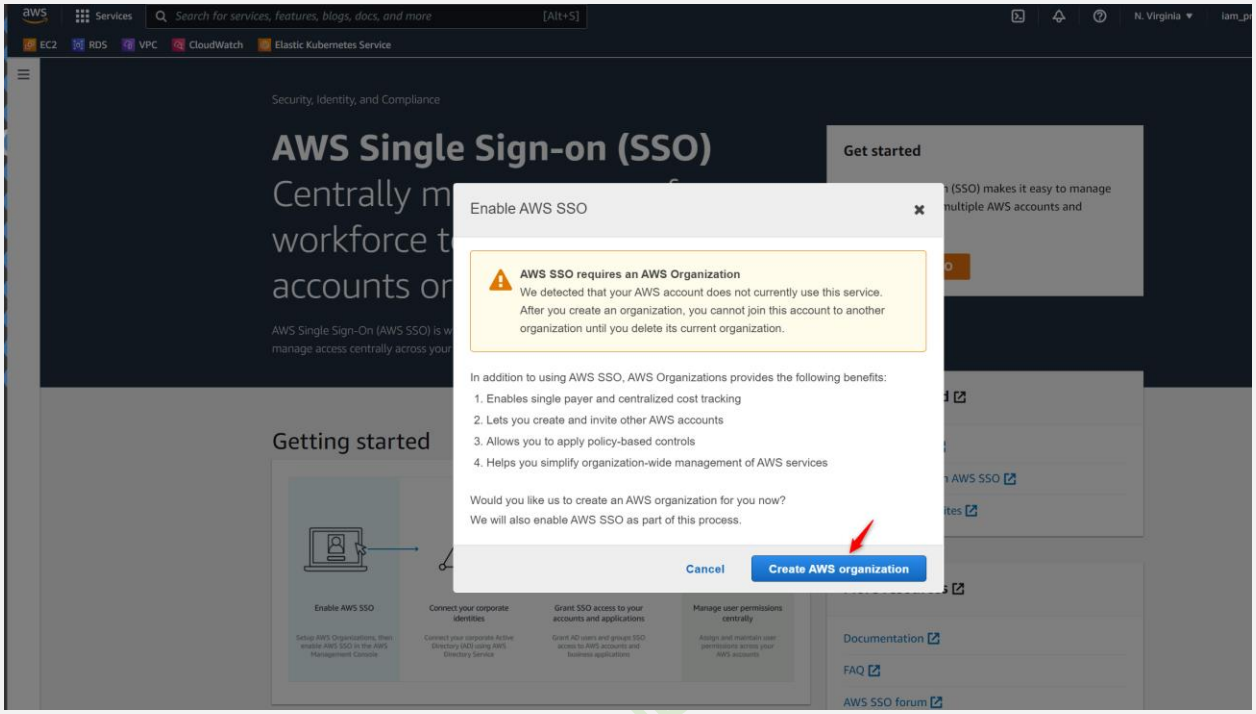
1. Log in to your AWS account and go to the Single Sign-On service.

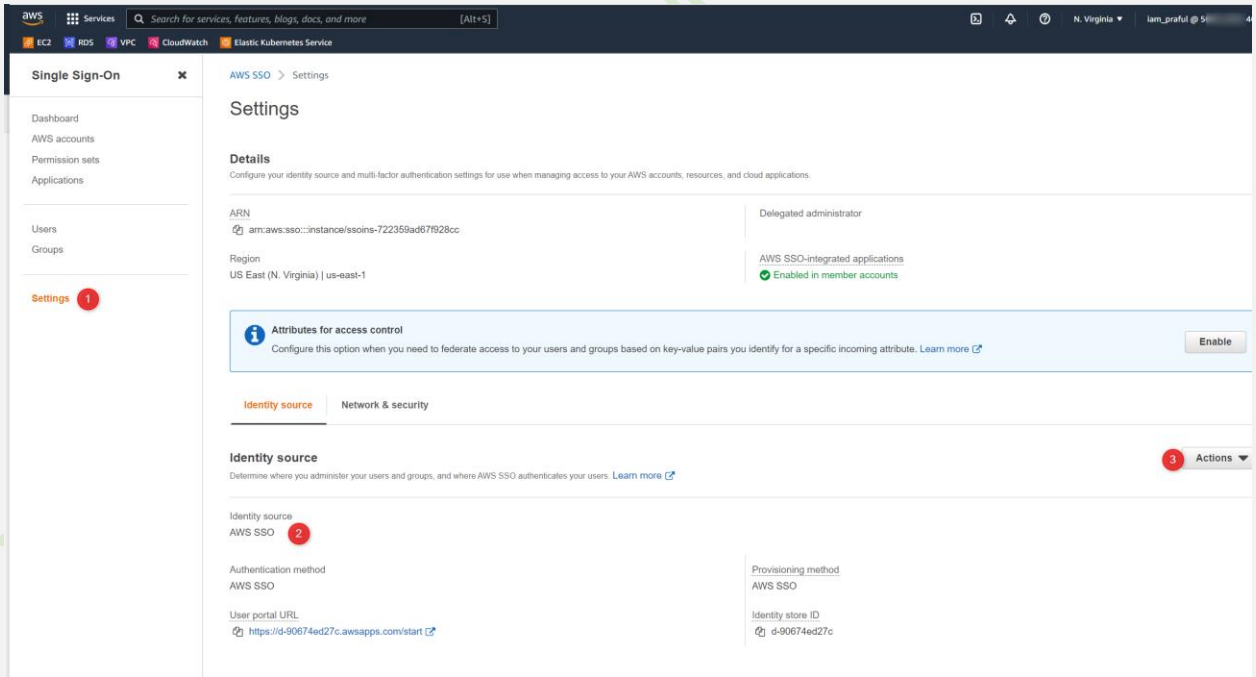


2. Within AWS SSO, go to the Settings page and choose Change in the Identity Source.



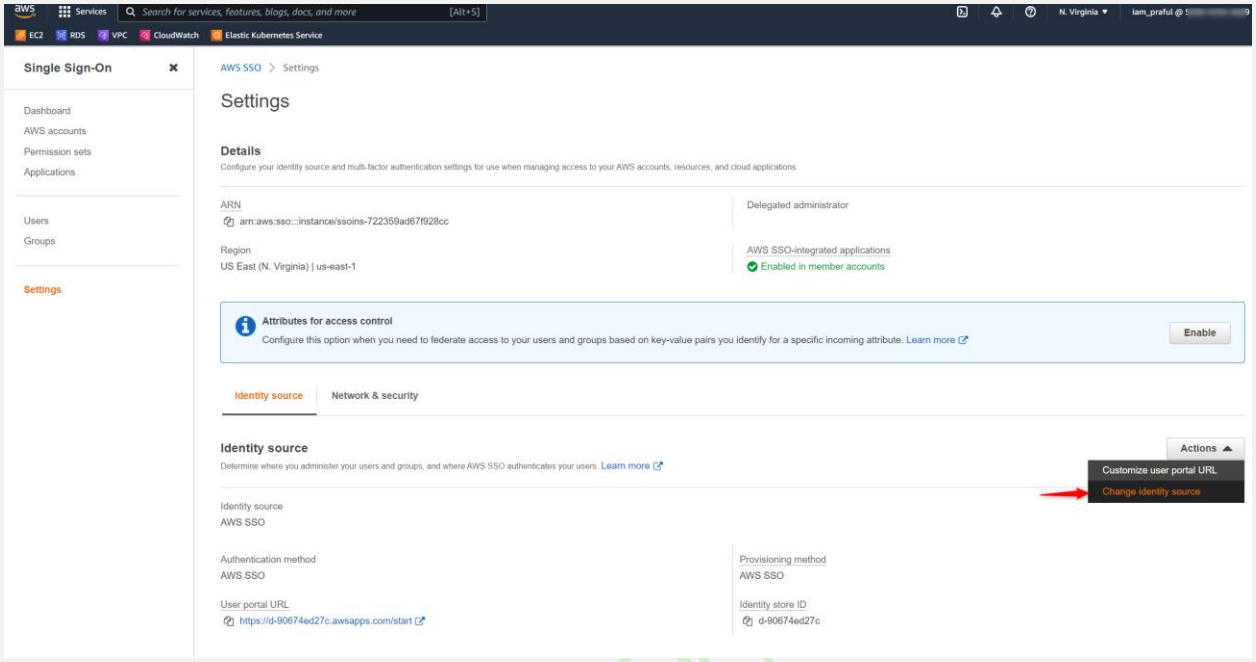
Create Organization



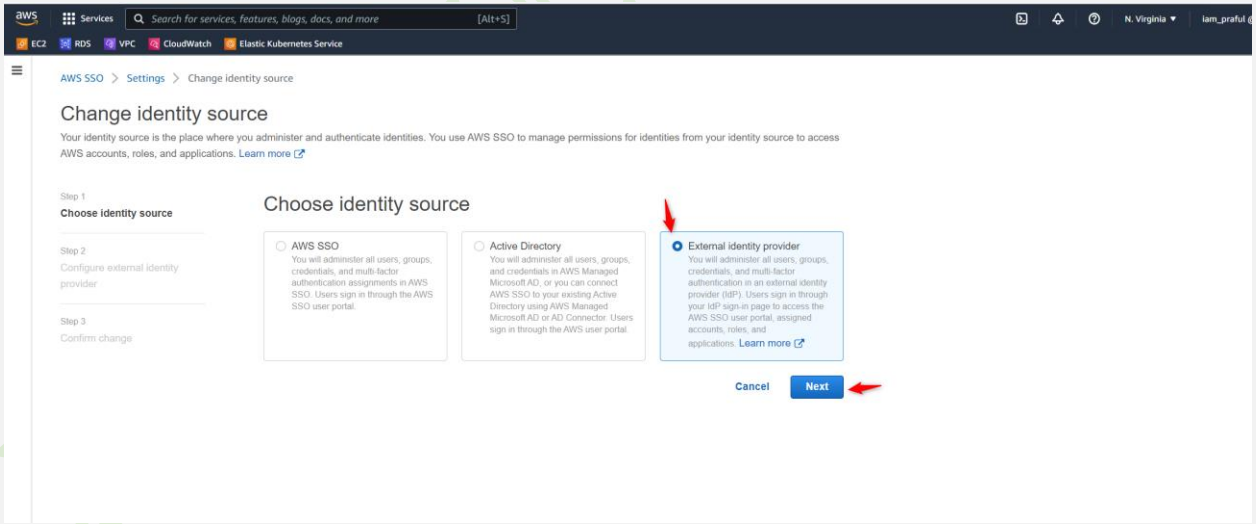


Click on Actions

Click change identity source

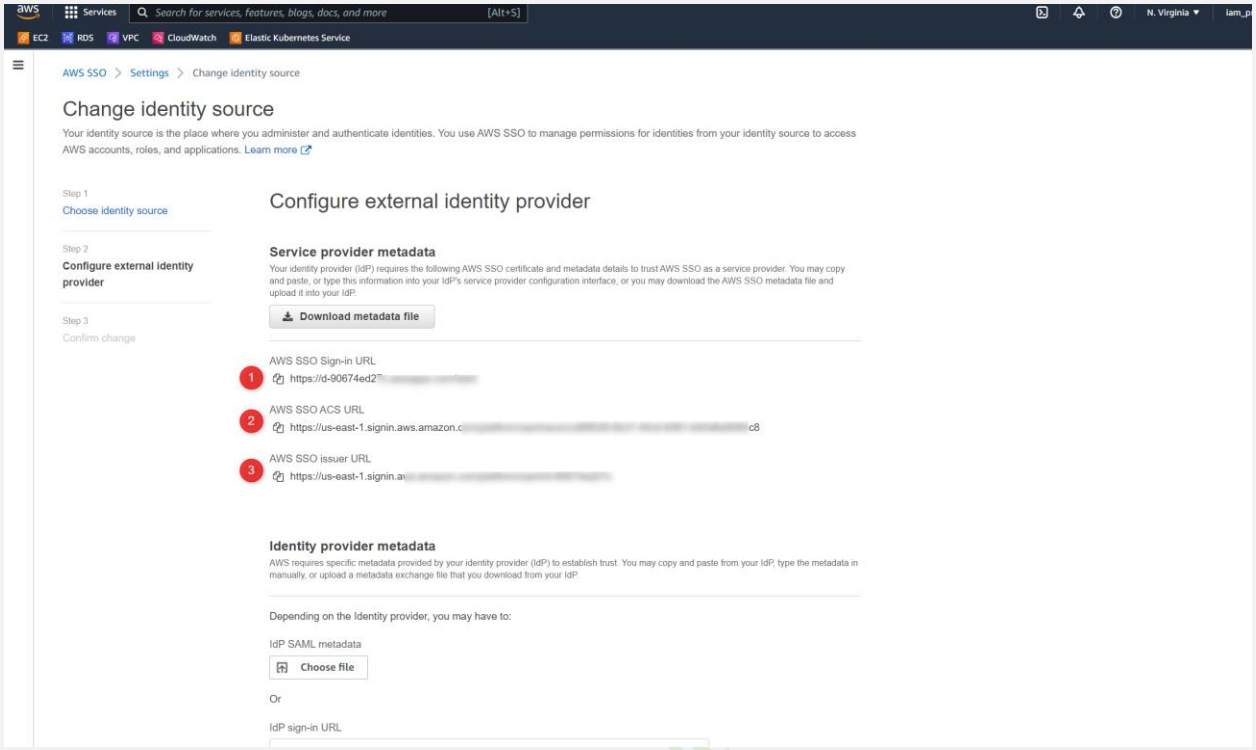


3. In the Change Identity Source page, choose External Identity Provider.



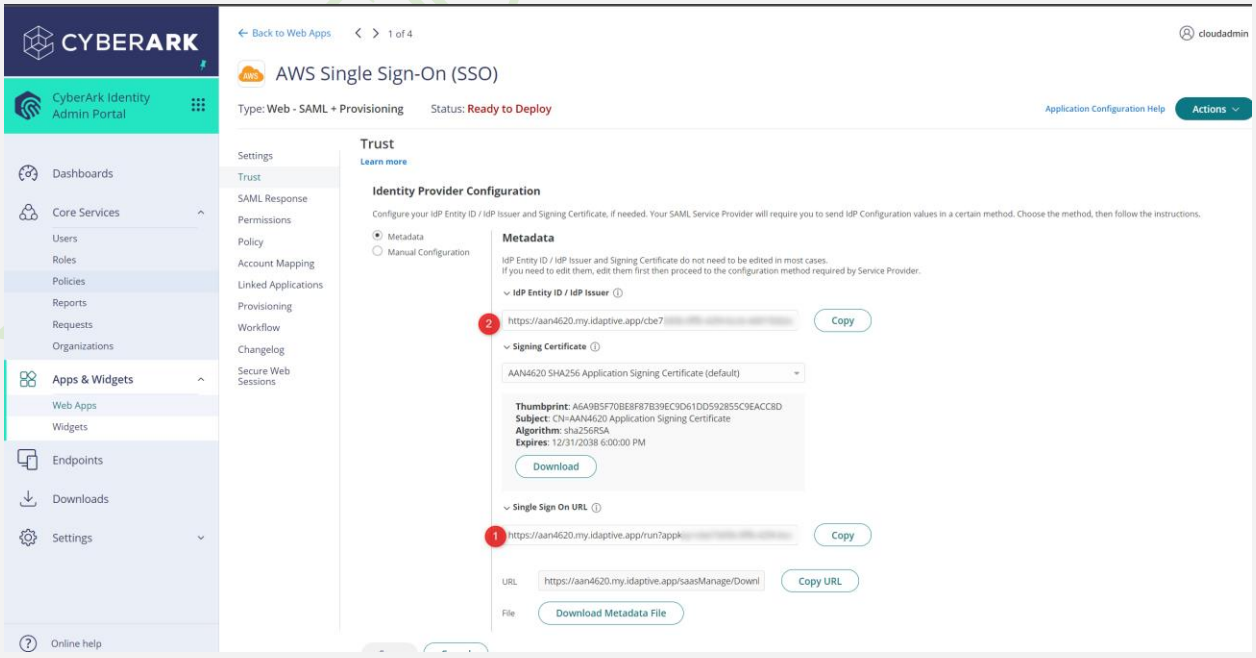
4. Under the Service provider metadata, expand the view to see all of the values and copy AWS SSO ACS URL and AWS SSO issuer URL to be used later in CyberArk AWS SSO application configuration.

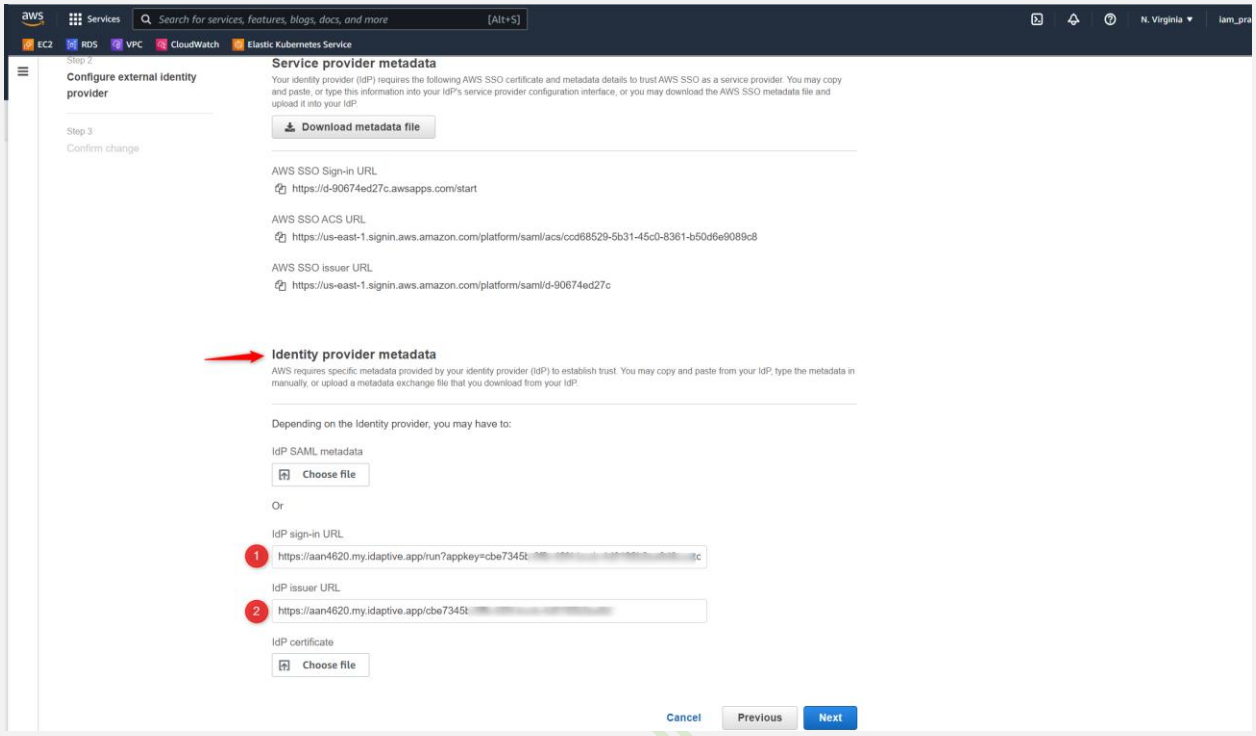
Service provider metadata:



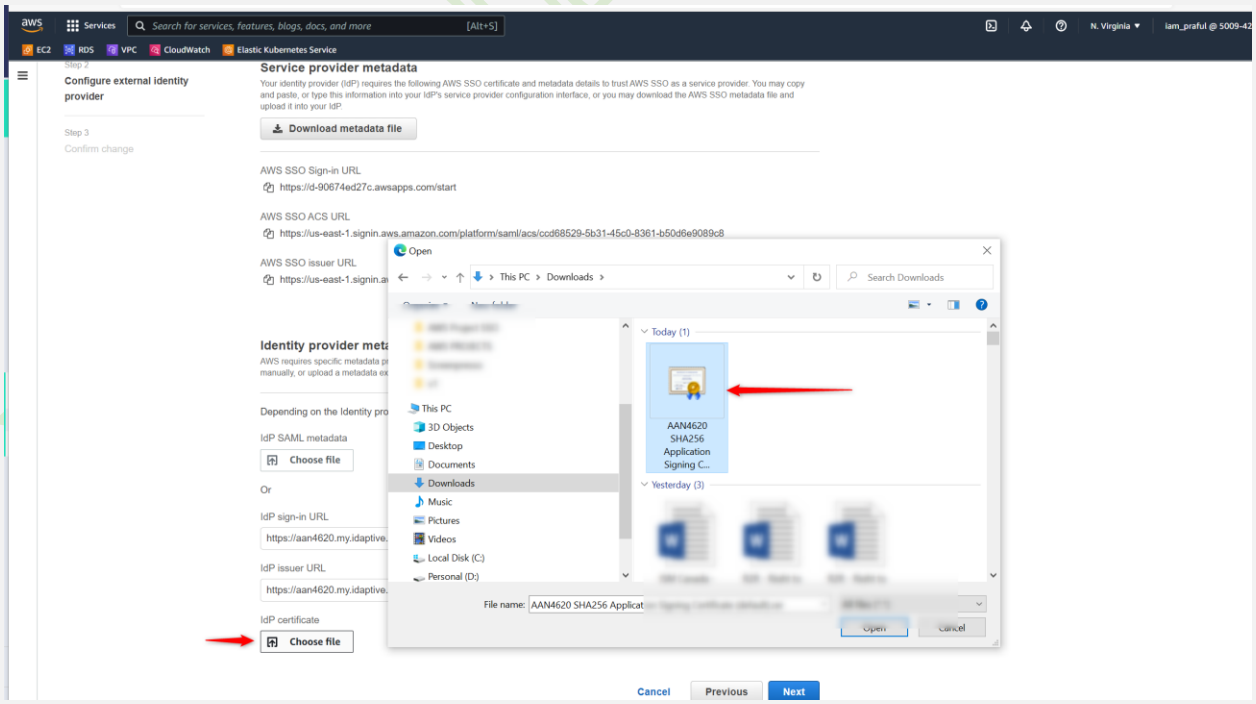
5. Under the Identity provider metadata section, paste the Single Sign-ON URL and IdP Entity ID you copied from CyberArk to the IdP sign-in URL and IdP issuer URL fields, respectively.

Identity provider metadata:

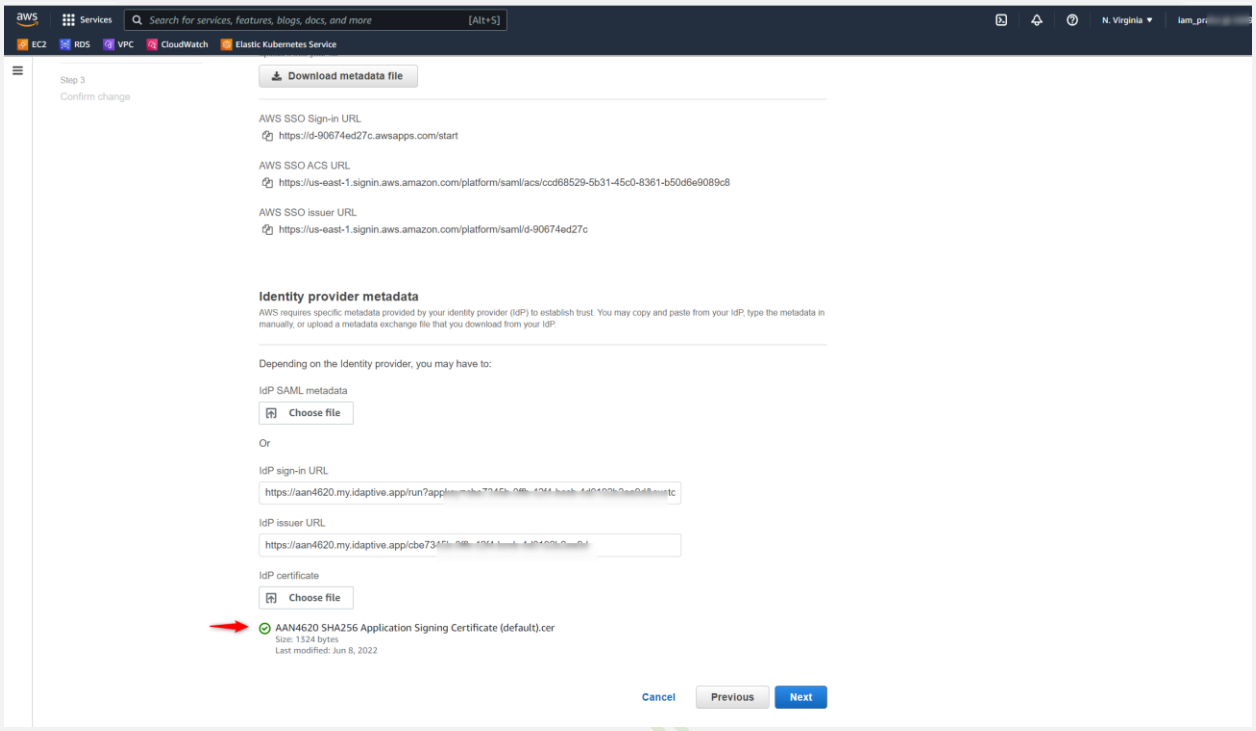


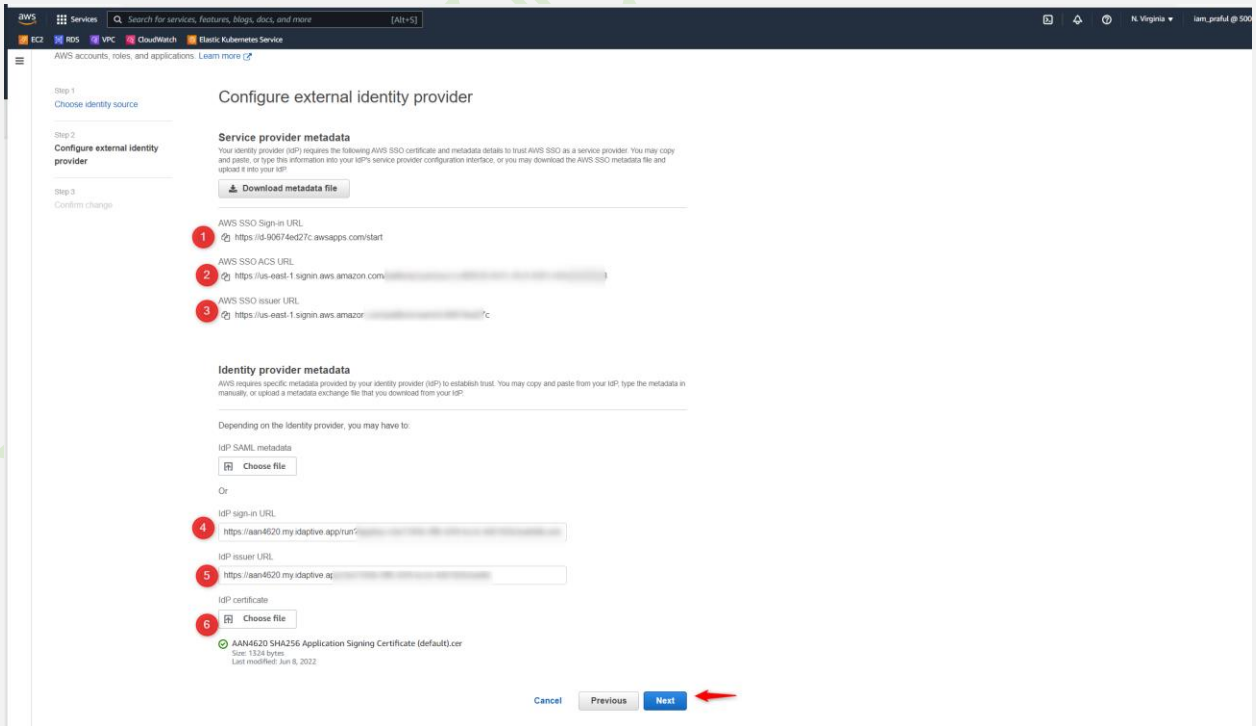


6. Upload the CyberArk certificate you downloaded earlier to the IdP certificate and then choose Next: Review.

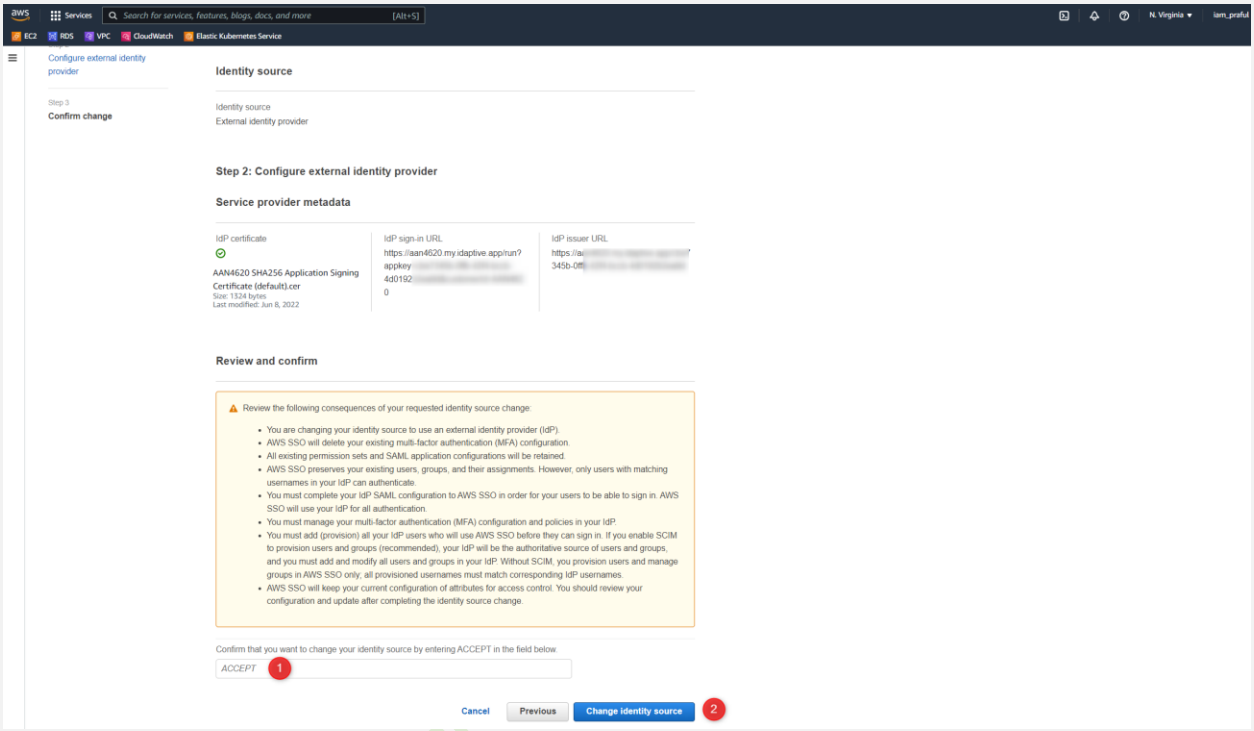


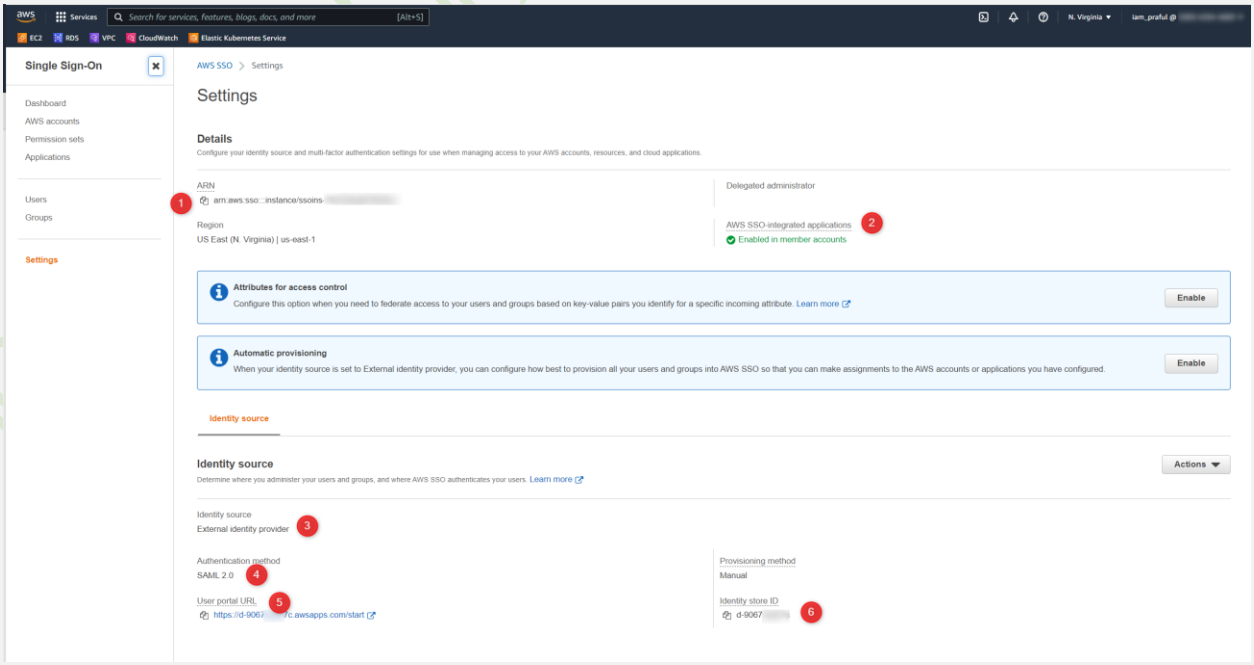
Certificate upload successful


Download metadata file
AWS SSO Sign-in URL
https://d-90674ed27c.awsapps.com/start
AWS SSO ACS URL
https://us-east-1.signin.aws.amazon.com/platform/saml/acs/ccd68529-5b31-45c0-8361-b50d6e9089c8
AWS SSO issuer URL
https://us-east-1.signin.aws.amazon.com/platform/saml/d-90674ed27c
Identity provider metadata
AWS requires specific metadata provided by your identity provider (IdP) to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.
Depending on the Identity provider, you may have to:
IdP SAML metadata
Choose file
Or
IdP sign-in URL
IdP issuer URL
IdP certificate
Choose file
AAN4620 SHA256 Application Signing Certificate (default).cer
Size: 1324 bytes
Last modified: Jun 8, 2022
Cancel
Previous
Next


Configure external identity provider
Service provider metadata
Download metadata file
1
2
3
Identity provider metadata
Depending on the Identity provider, you may have to:
IdP SAML metadata
Choose file
Or
IdP sign-in URL
4
IdP issuer URL
5
IdP certificate
6
Choose file
AAN4620 SHA256 Application Signing Certificate (default).cer
Cancel
Previous
Next

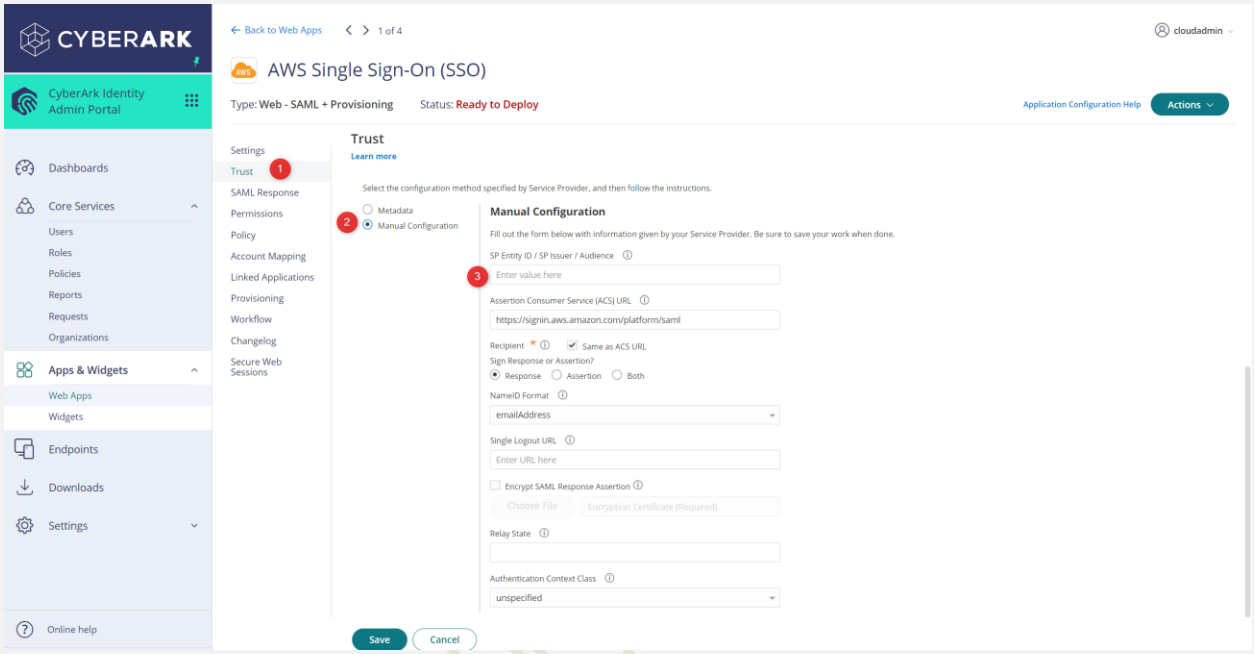
7. On the next screen, type ACCEPT to Changes identity source.



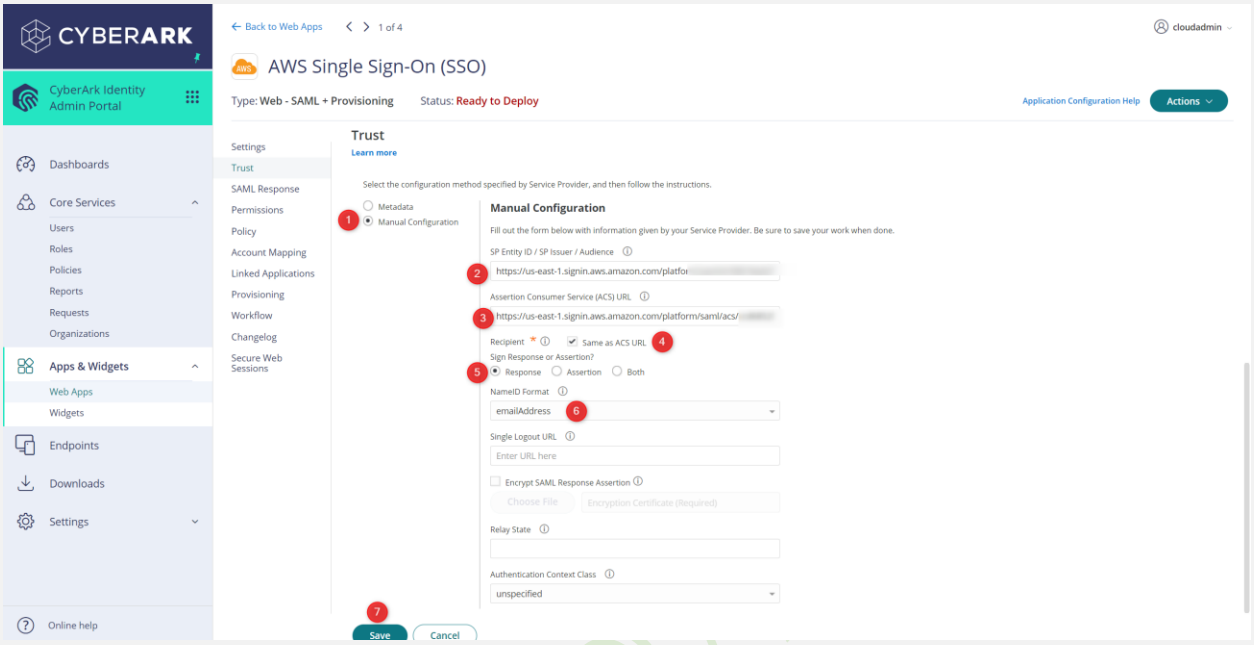


CyberArk Workforce Identity – Configuring AWS SSO Application

1. Back in the CyberArk admin portal where you have the AWS SSO app configured, under the Trust section go to the Service Provider Configuration and choose Manual Configuration.

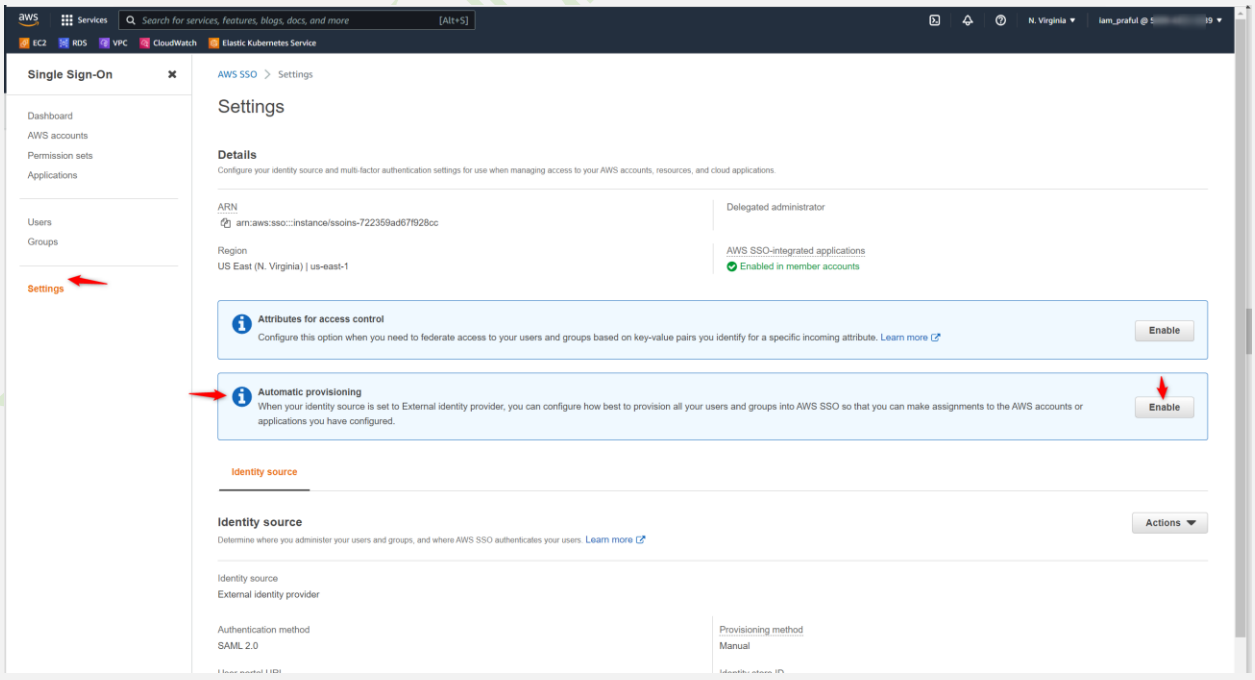


2. Paste the AWS SSO issuer URL you copied from AWS SSO in the SP Entity ID/ SP Issuer/Audience field
3. Paste the AWS SSO CS URL you copied from AWS SSO in the Assertion Consumer Service (ACS) URL field.
4. The Recipient field should be the same as the ACS URL.
5. Make sure the NameID Format is set to emailAddress.
6. Choose Save Settings.

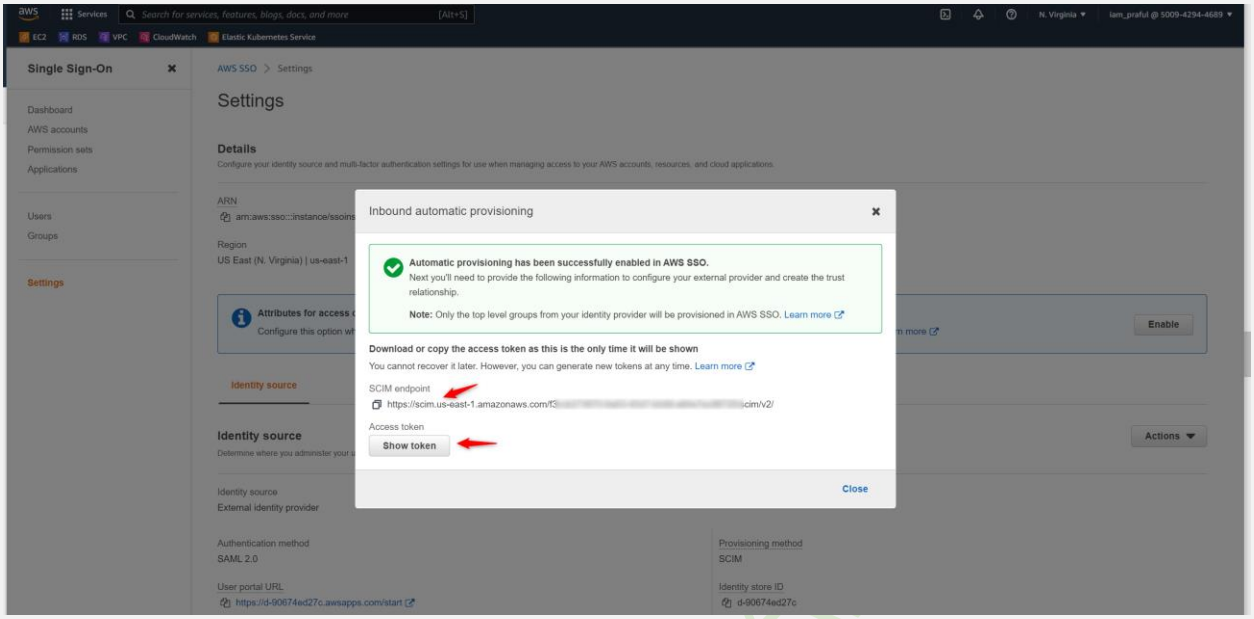


AWS SSO – Setting Up SCIM

1. In AWS SSO, go to the Settings page and choose Enable automatic provisioning.

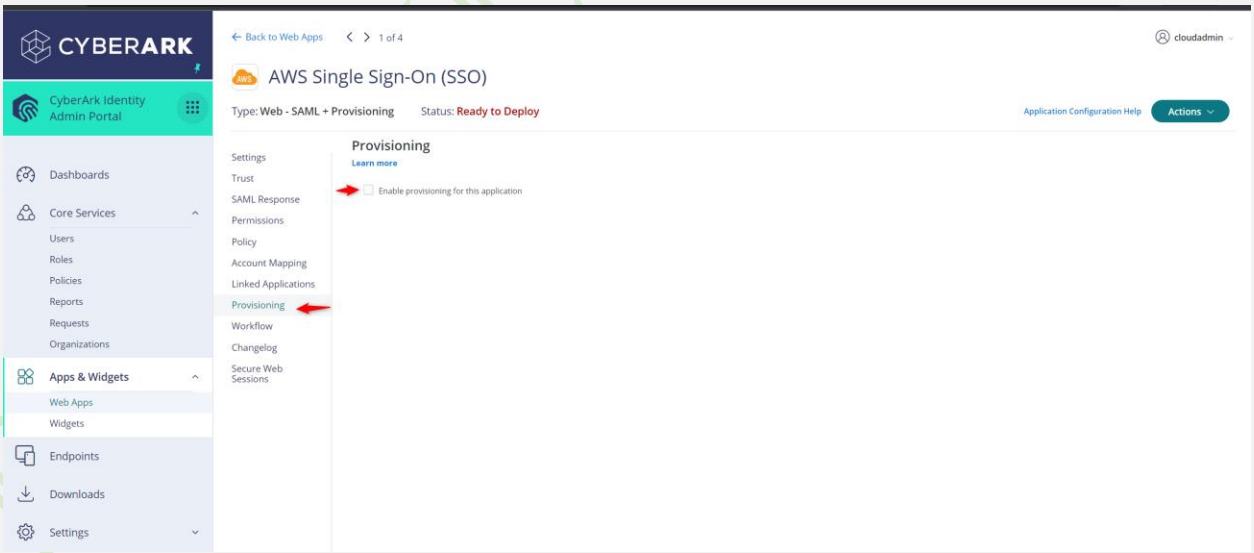


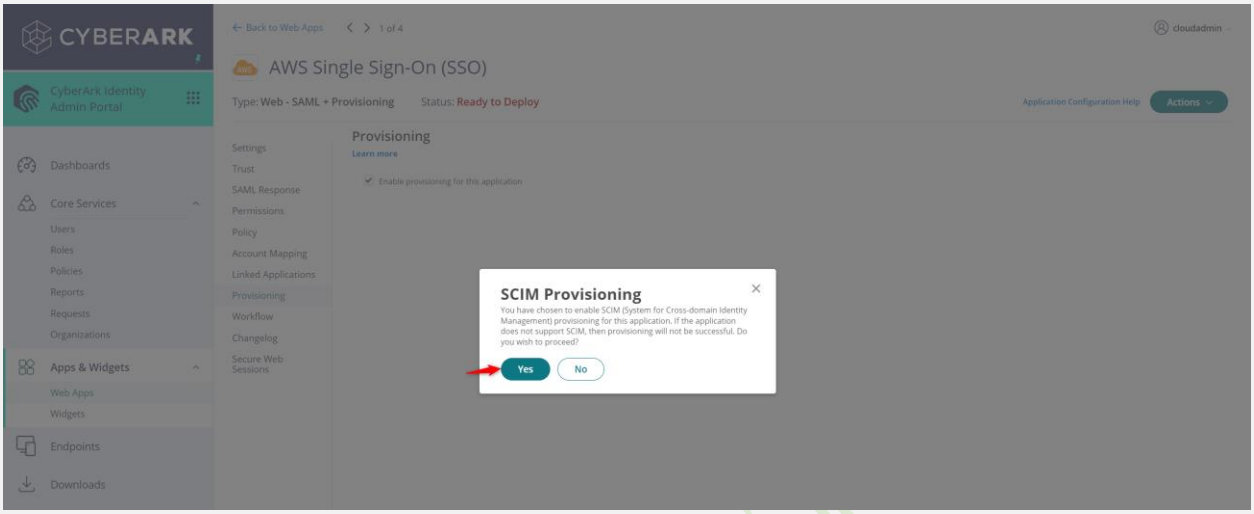
2. Copy the SCIM endpoint and Access token; note that after closing this window the Access token cannot be viewed again and a new key will be needed.



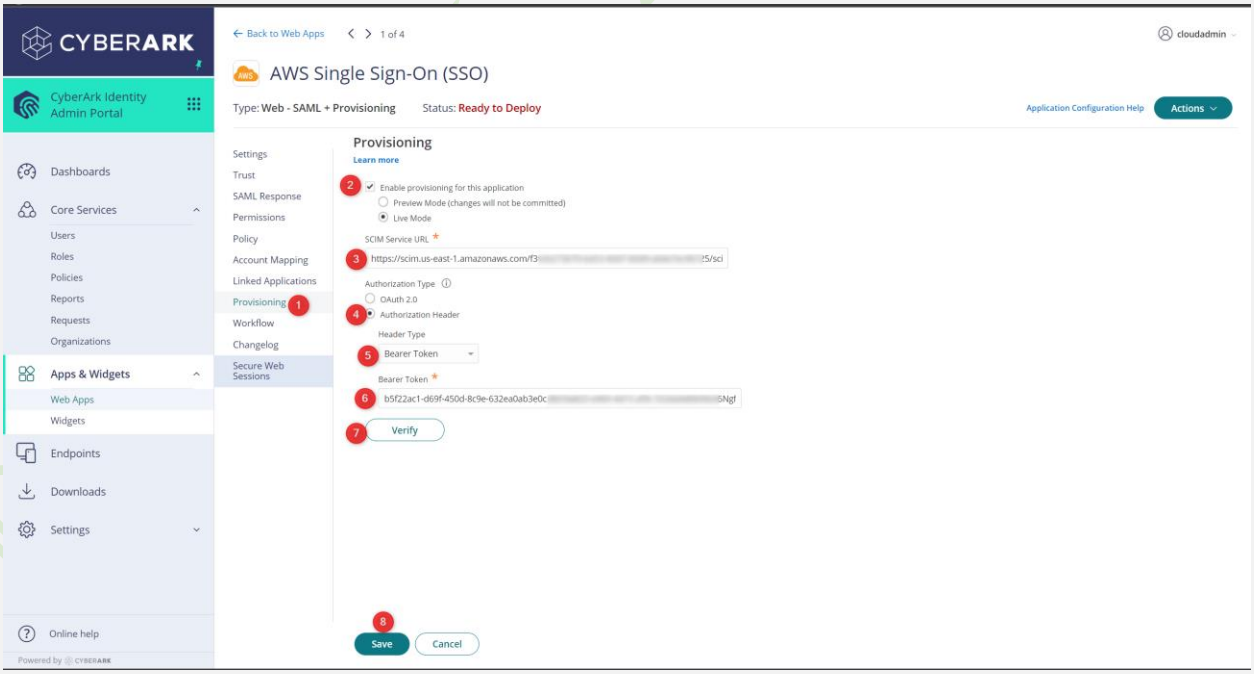
CyberArk Workforce Identity – Configuring SCIM

1. Return to the CyberArk Workforce Identity admin portal. Go to the Provisioning tab and check the box to Enable Provisioning for this application.

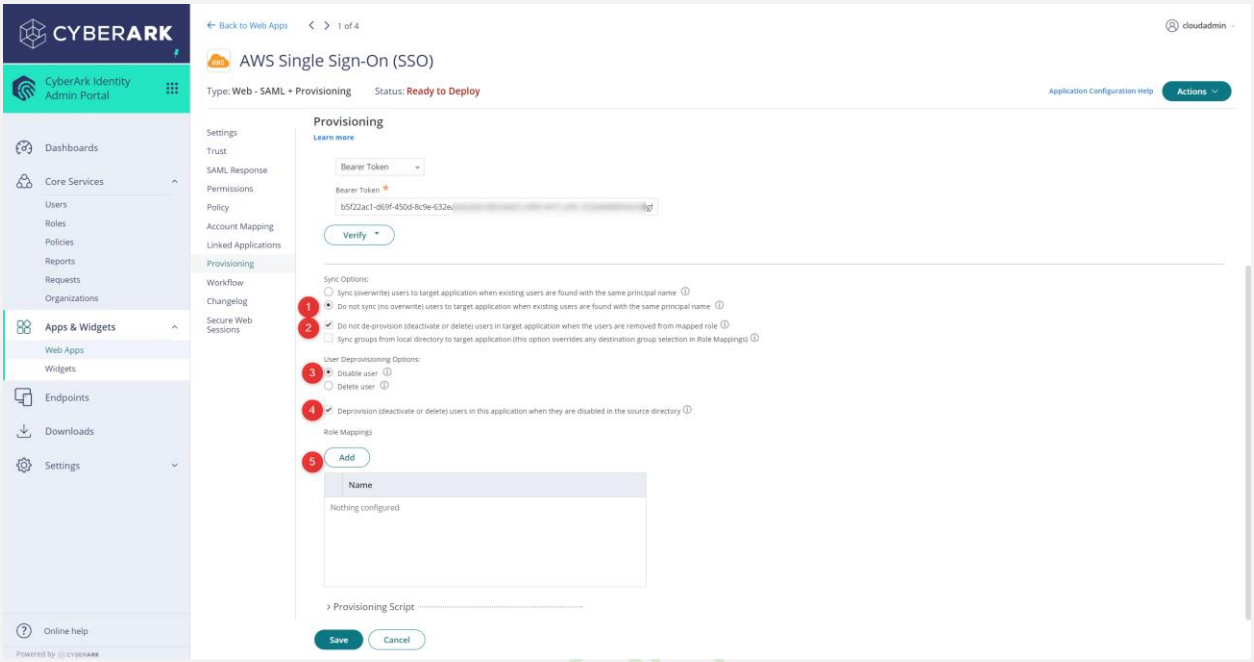




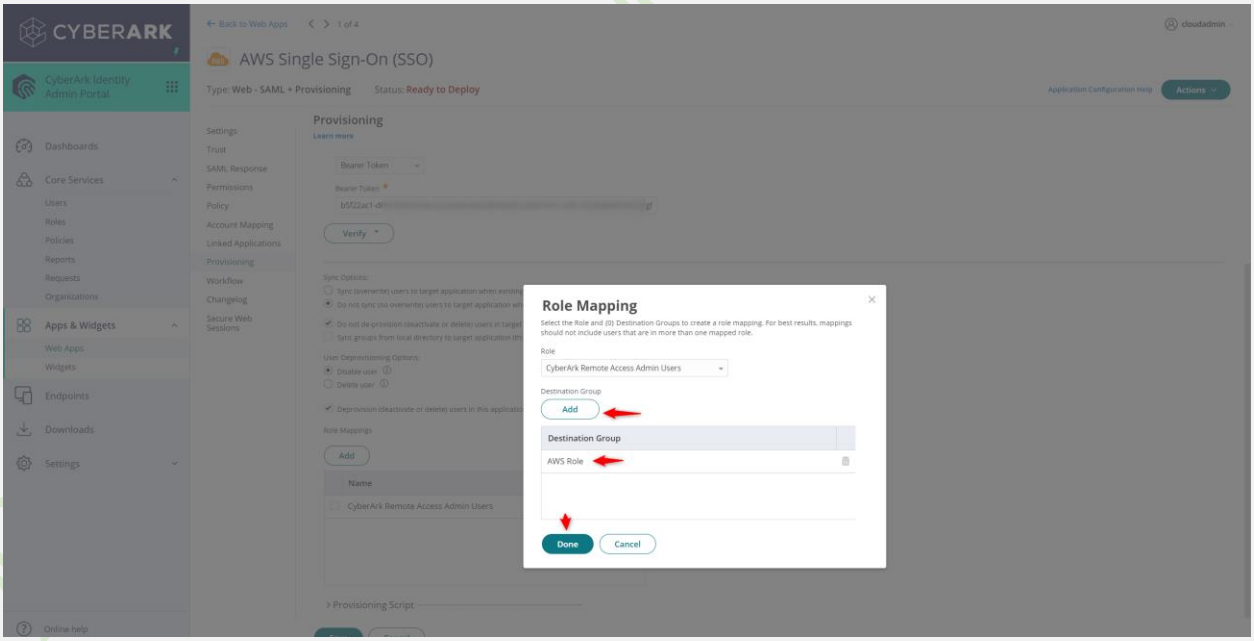
2. Make sure the Authentication Type is Authorization Header and the Header Type is Bearer Token.
3. Paste the SCIM endpoint from AWS SSO in the SCIM service URL field. *Important:* Make sure to remove the trailing "/".
4. Paste the Access token from AWS SSO in the Bearer Token field.
5. Choose Verify to make sure the setting is correct and the link is up.



6. At the bottom of the Provisioning page you can choose your sync options and add Role Mapping.

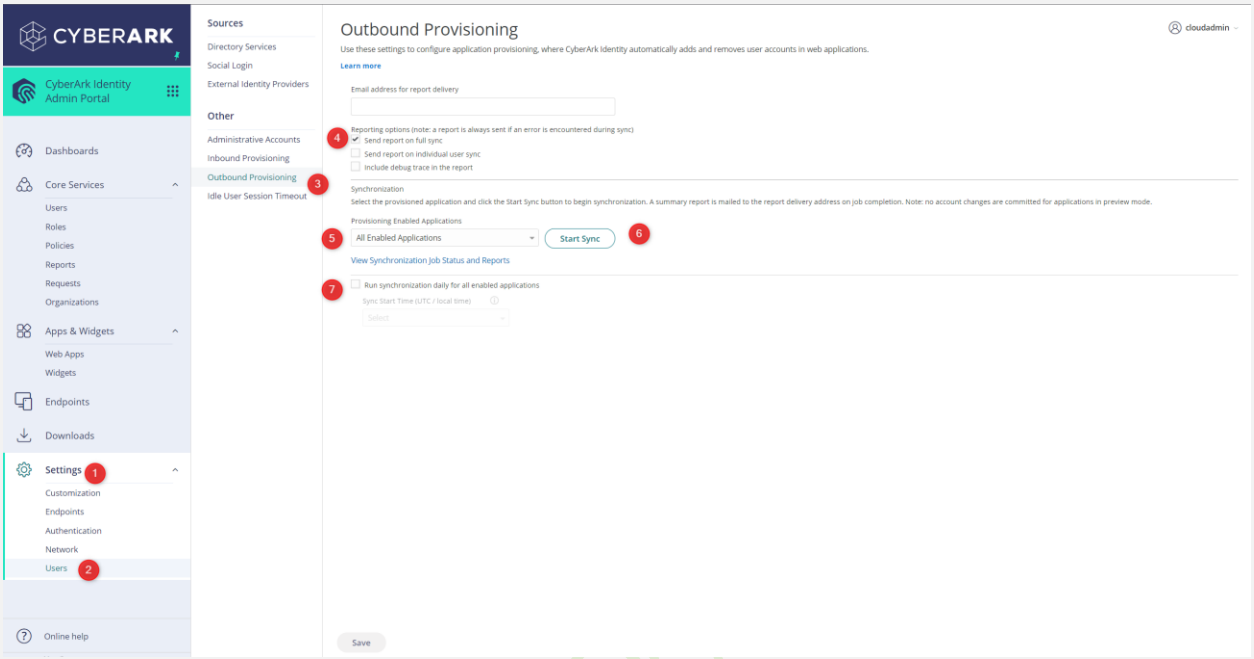


Add Role: AWS Role

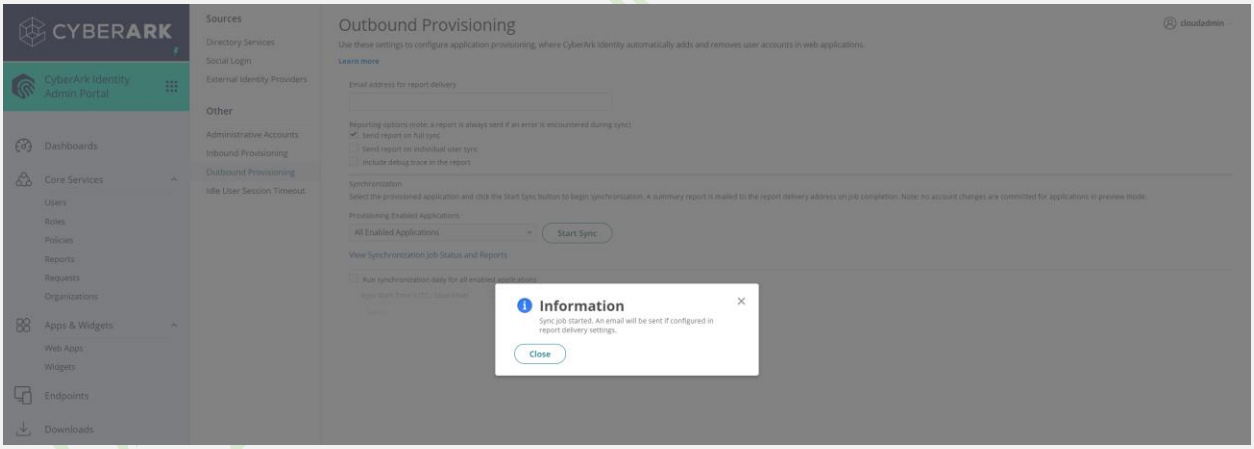


Go to Settings

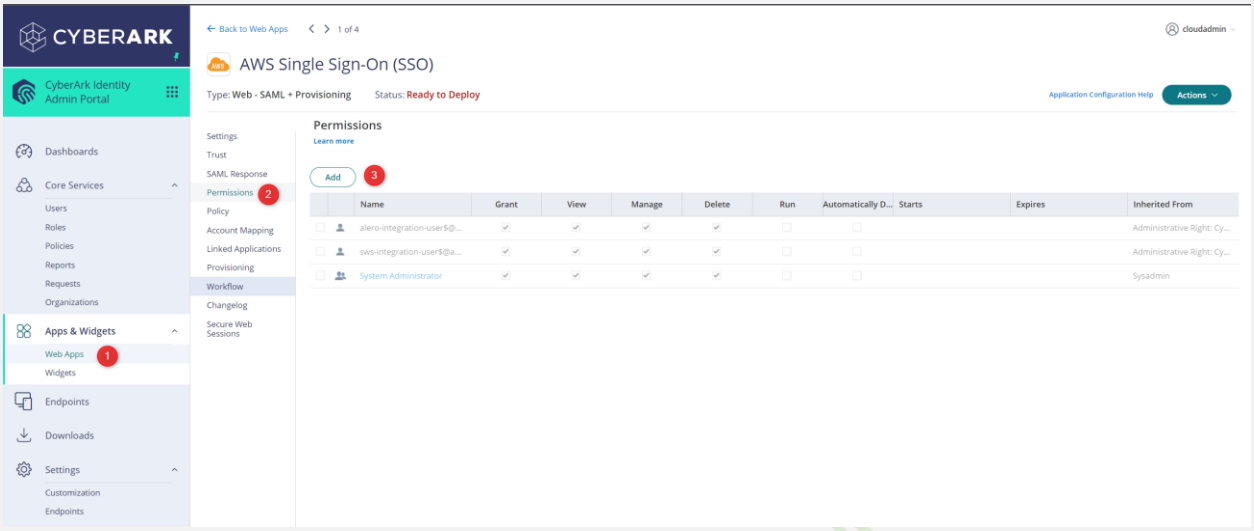
Users



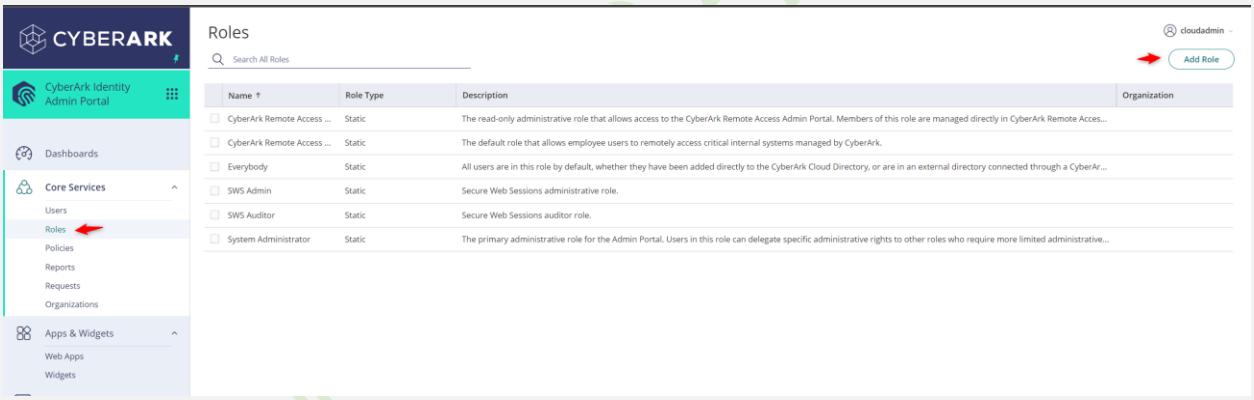
Sync start

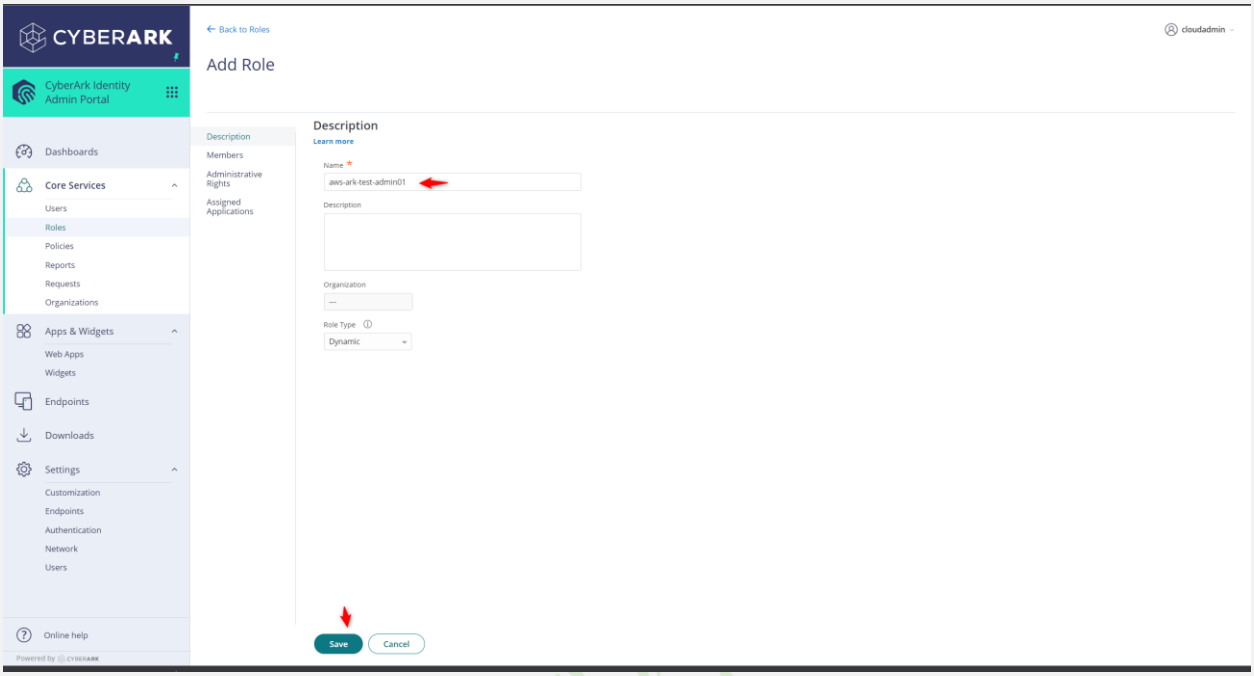


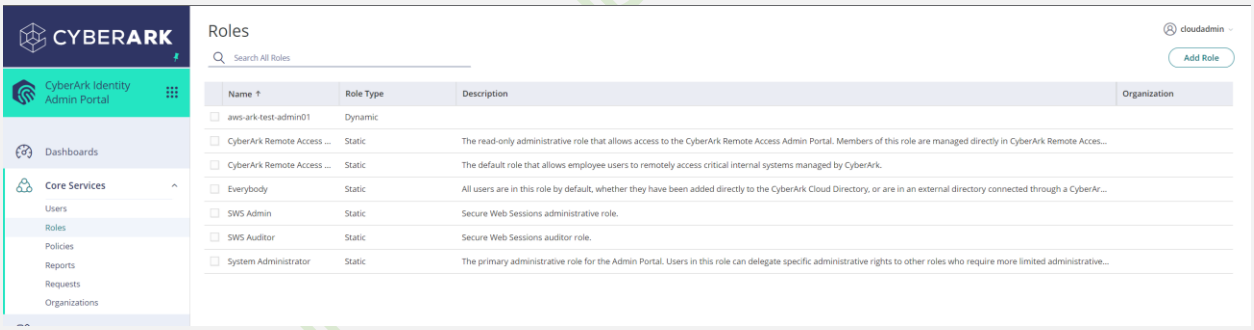
11. Lastly, to deploy and enable this new application you need to assign it to certain roles or users. Go to the Permissions tab and choose Add.
12. Search and choose which users and roles you want to have permissions for this application and then Add them.



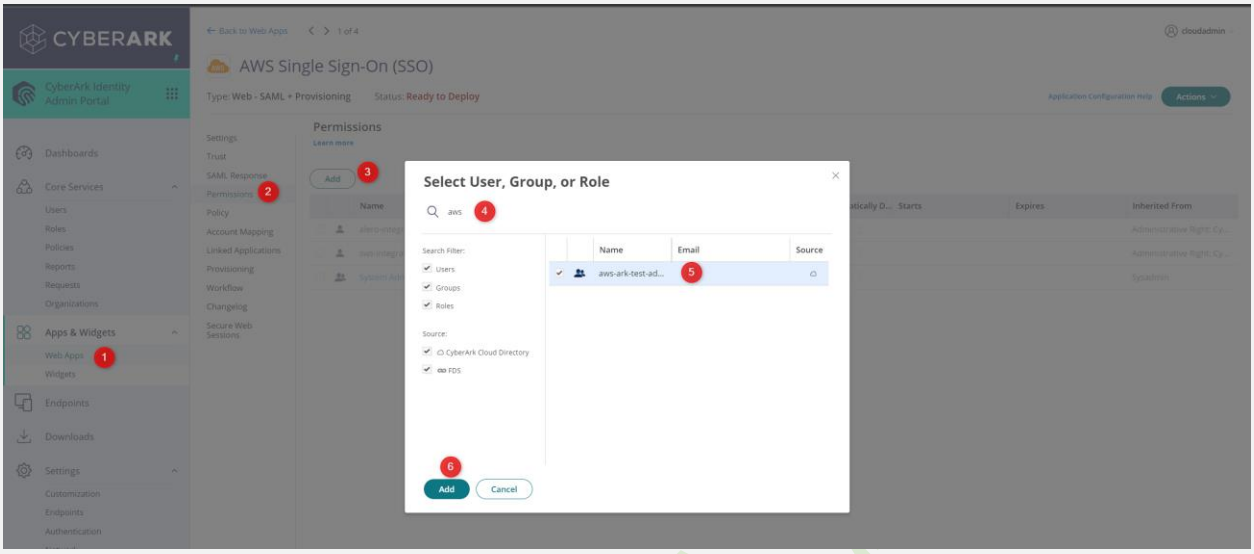
Create a new role

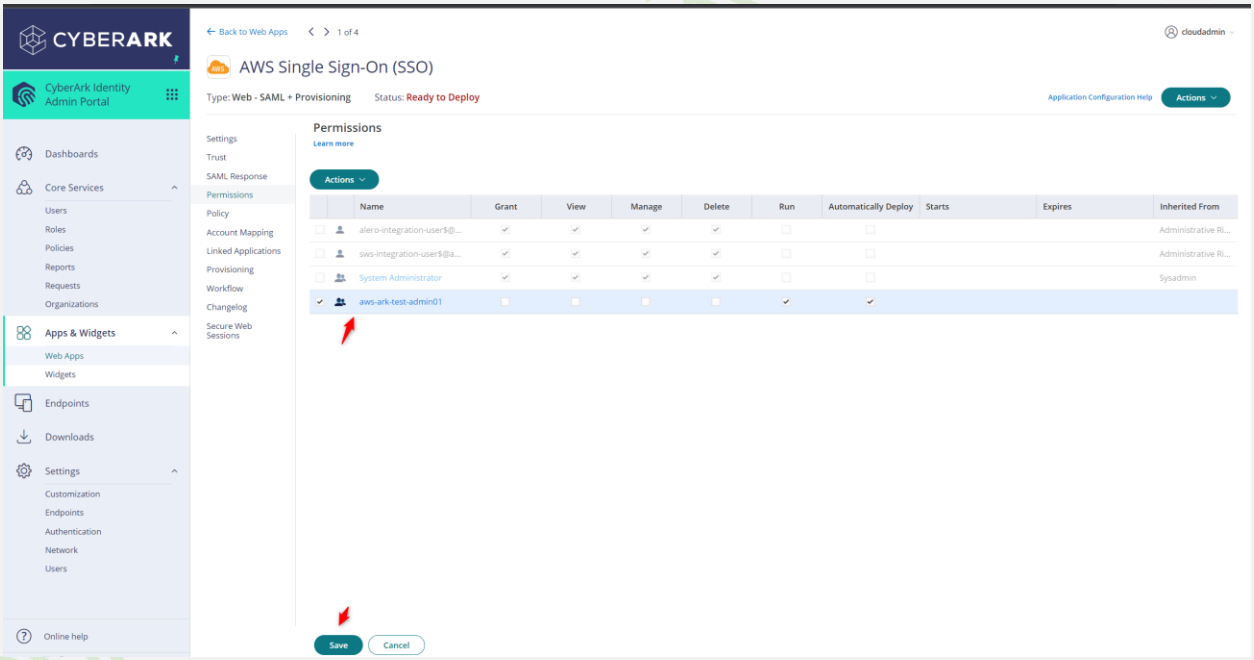




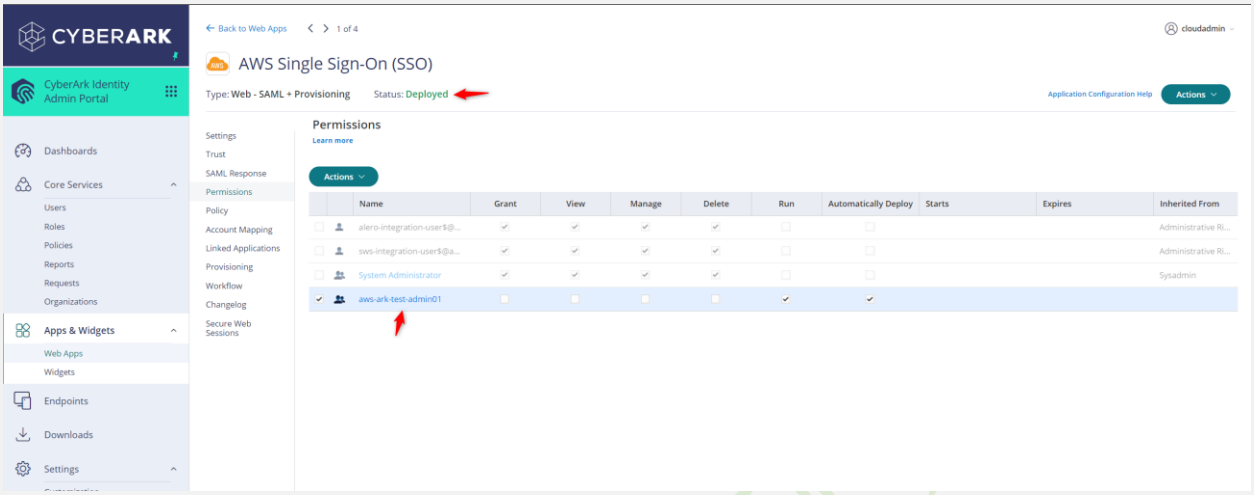


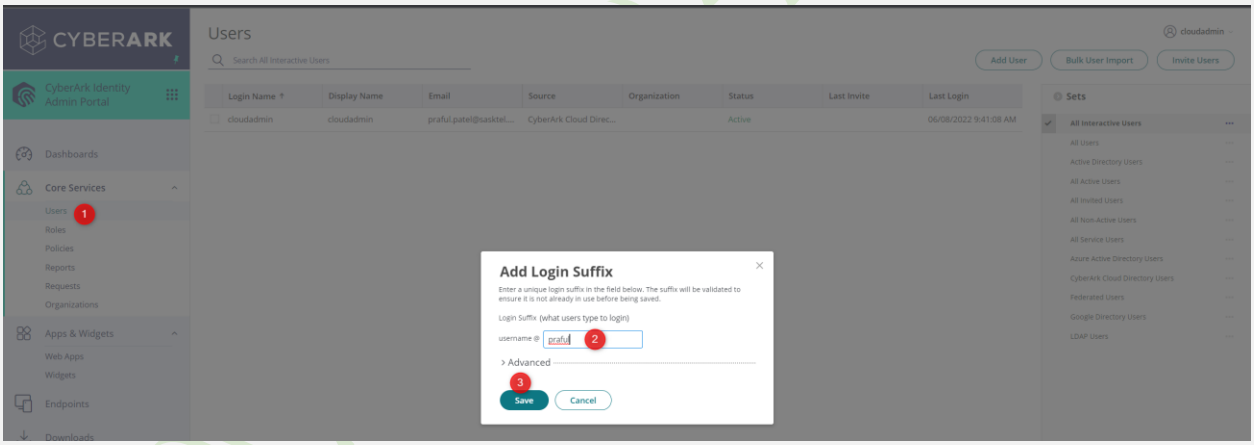
Add role to AWS SSO

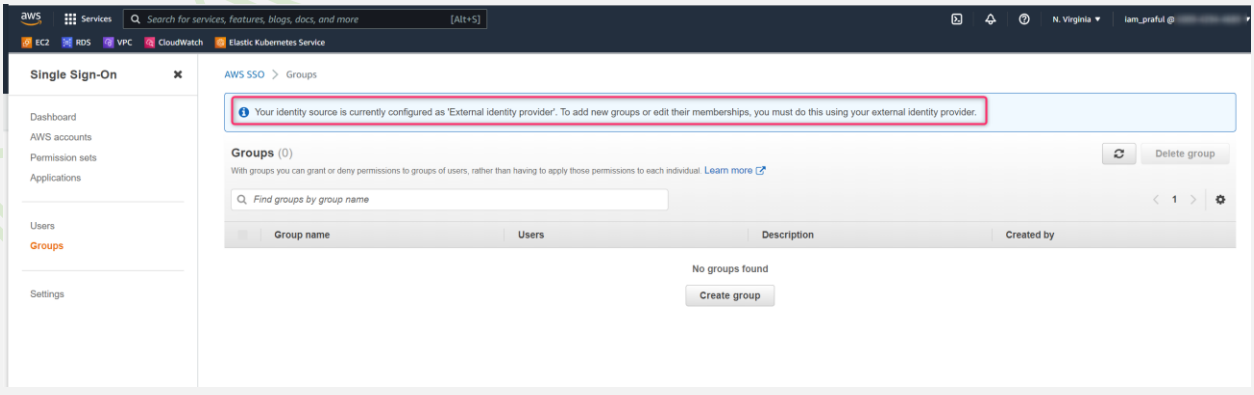


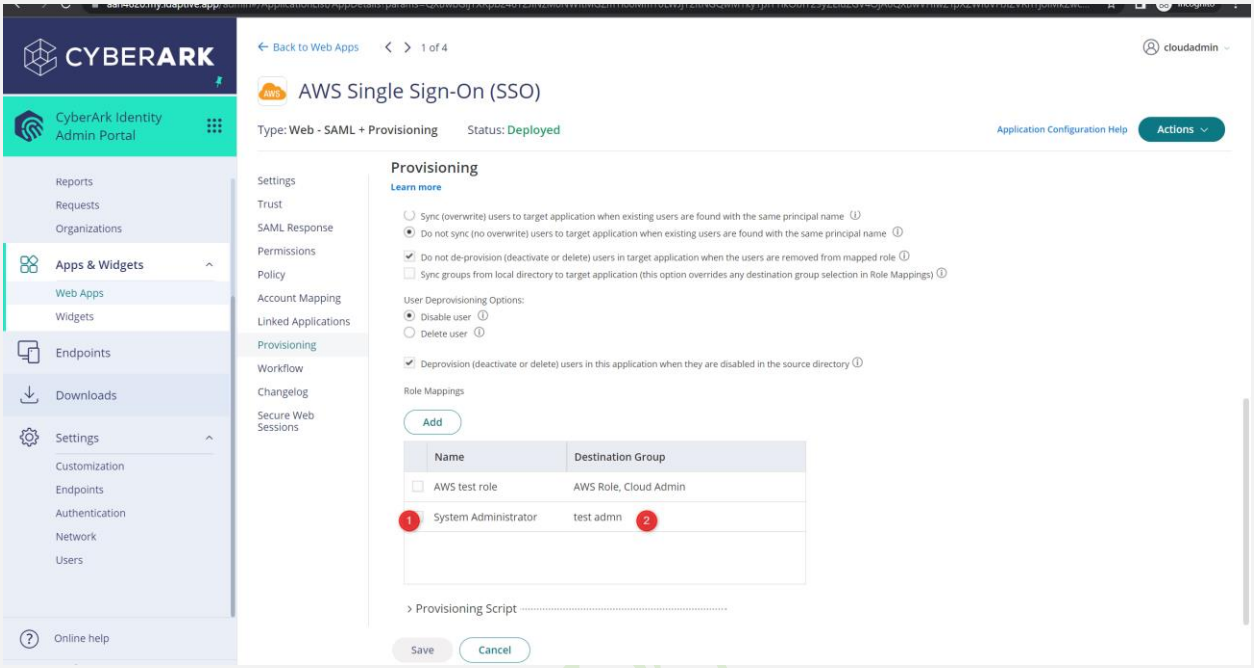


13. Once this step is completed you'll see the status change from Ready to Deploy to Deployed

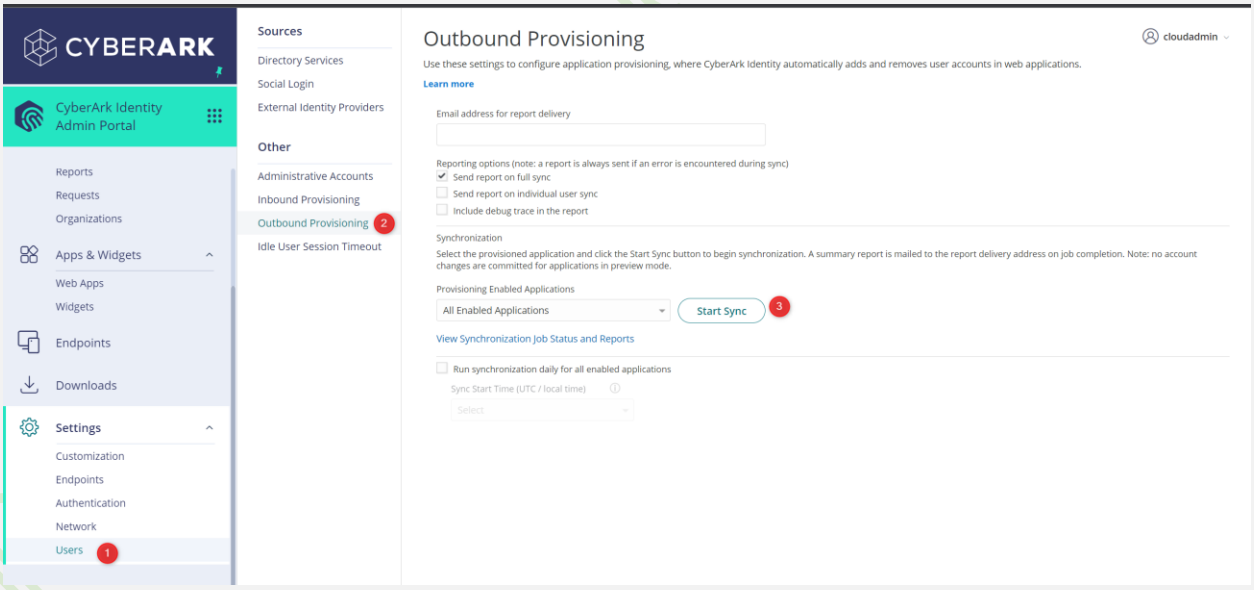

CYBERARK
CyberArk Identity Admin Portal
Back to Web Apps
1 of 4
cloudadmin
AWS Single Sign-On (SSO)
Type: Web - SAML + Provisioning
Status: Deployed
Application Configuration Help
Actions
Dashboards
Core Services
Users
Roles
Policies
Reports
Requests
Organizations
Apps & Widgets
Web Apps
Widgets
Endpoints
Downloads
Settings
Permissions
Learn more
Settings
Trust
SAML Response
Permissions
Policy
Account Mapping
Linked Applications
Provisioning
Workflow
Changelog
Secure Web Sessions
Name
Grant
View
Manage
Delete
Run
Automatically Deploy
Starts
Expires
Inherited From
aws-ark-test-admin01


CYBERARK
Users
Add User
Bulk User Import
Invite Users
Add Login Suffix
Enter a unique login suffix in the field below. The suffix will be validated to ensure it is not already in use before being saved.
Login Suffix (what users type to login)
username @ praful
Advanced
Save
Cancel
Sets

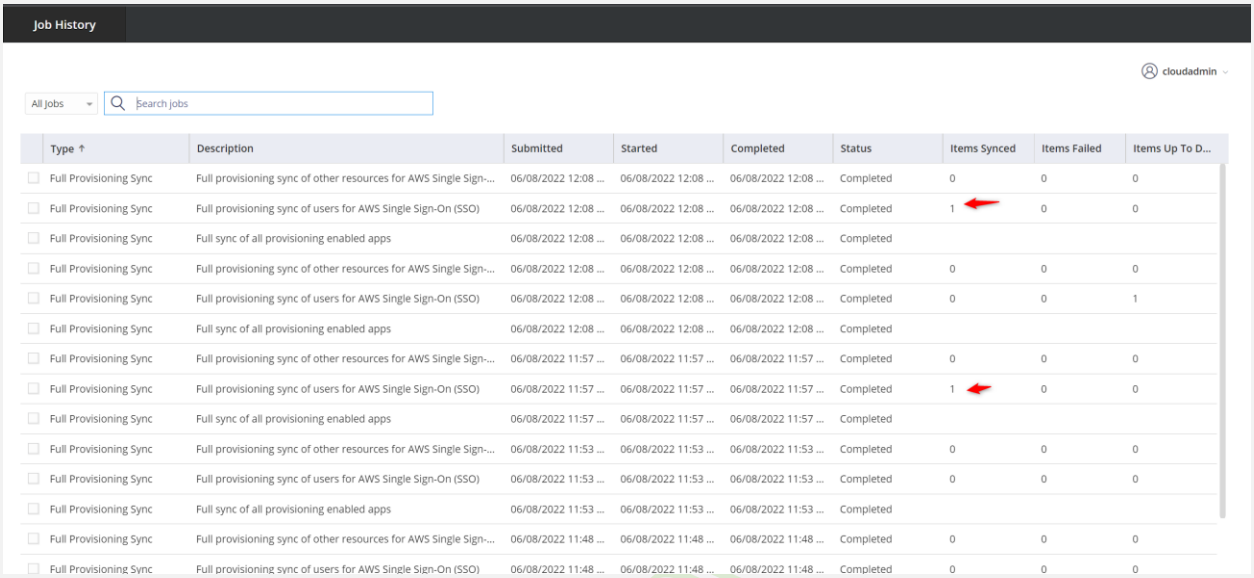

Single Sign-On
Dashboard
AWS accounts
Permission sets
Applications
Users
Groups
Settings
AWS SSO > Groups
Your identity source is currently configured as 'External identity provider'. To add new groups or edit their memberships, you must do this using your external identity provider.
Groups (0)
With groups you can grant or deny permissions to groups of users, rather than having to apply those permissions to each individual. Learn more
Delete group
Find groups by group name
Group name
Users
Description
Created by
No groups found
Create group



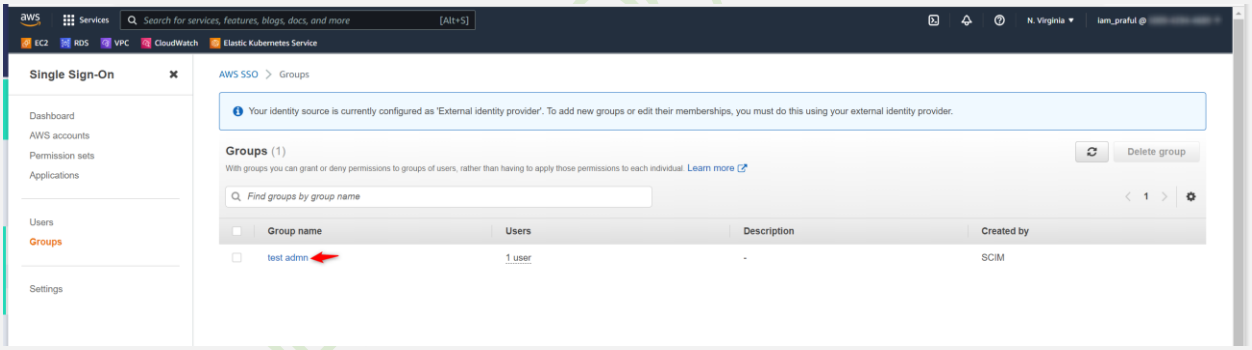
Click on Sync

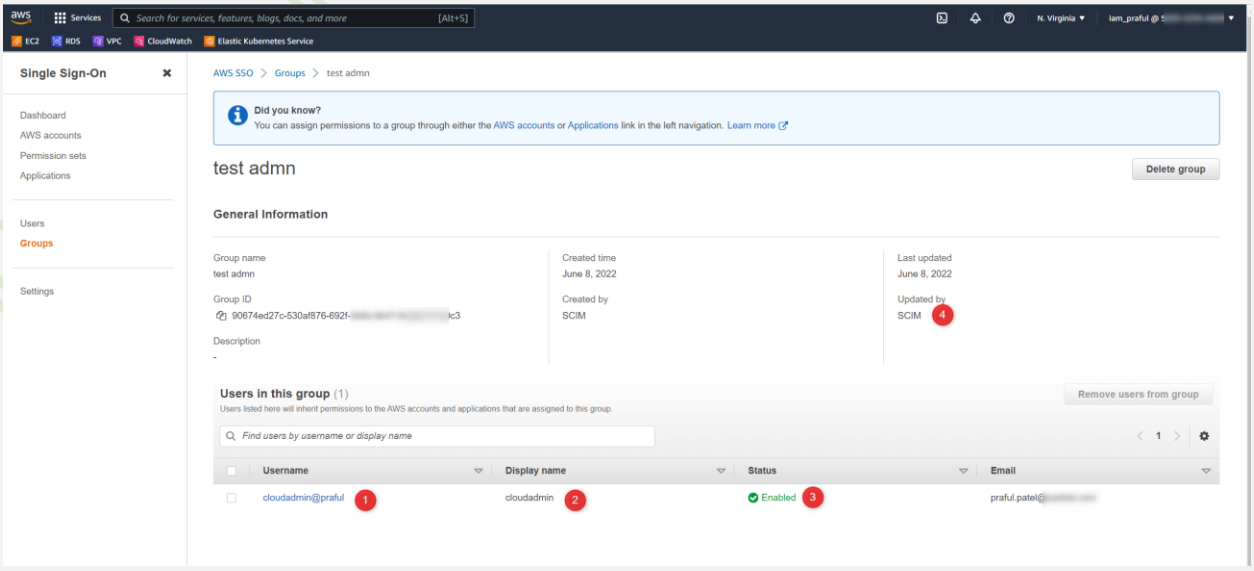


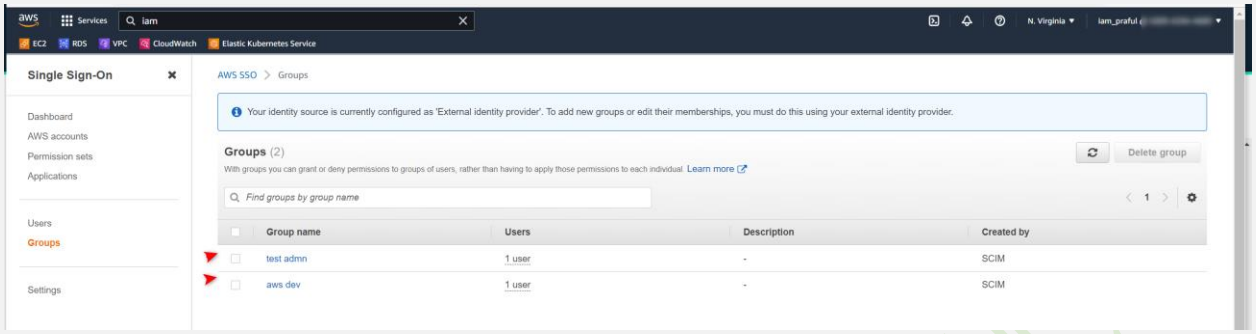
Verify sync status

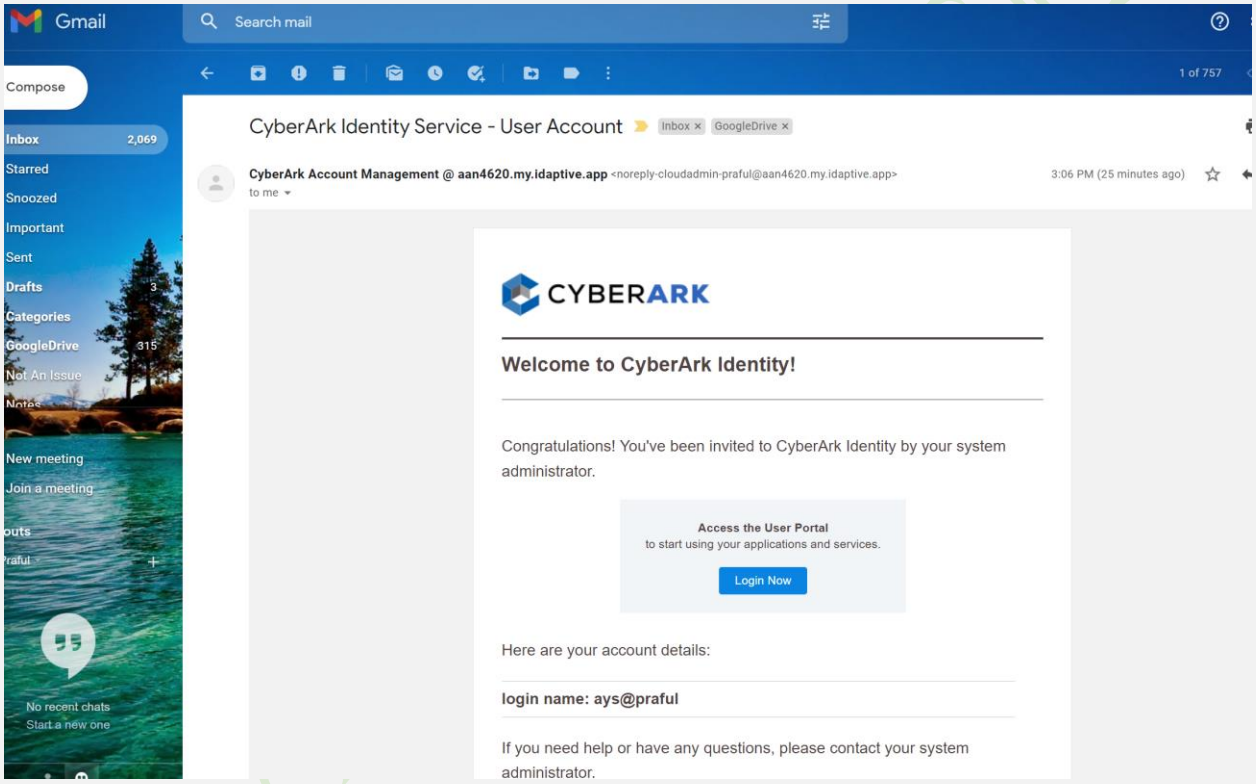


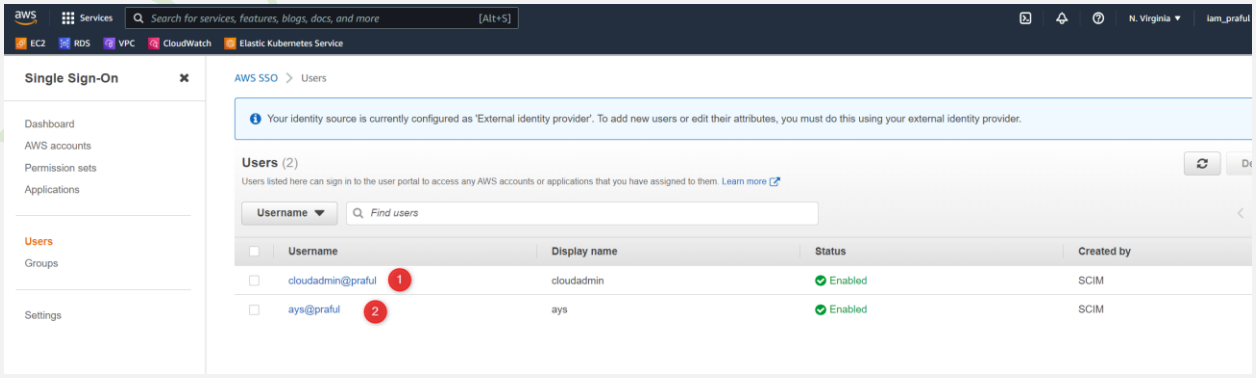
AWS Group – Test that group from cyberark Is synced with AWS

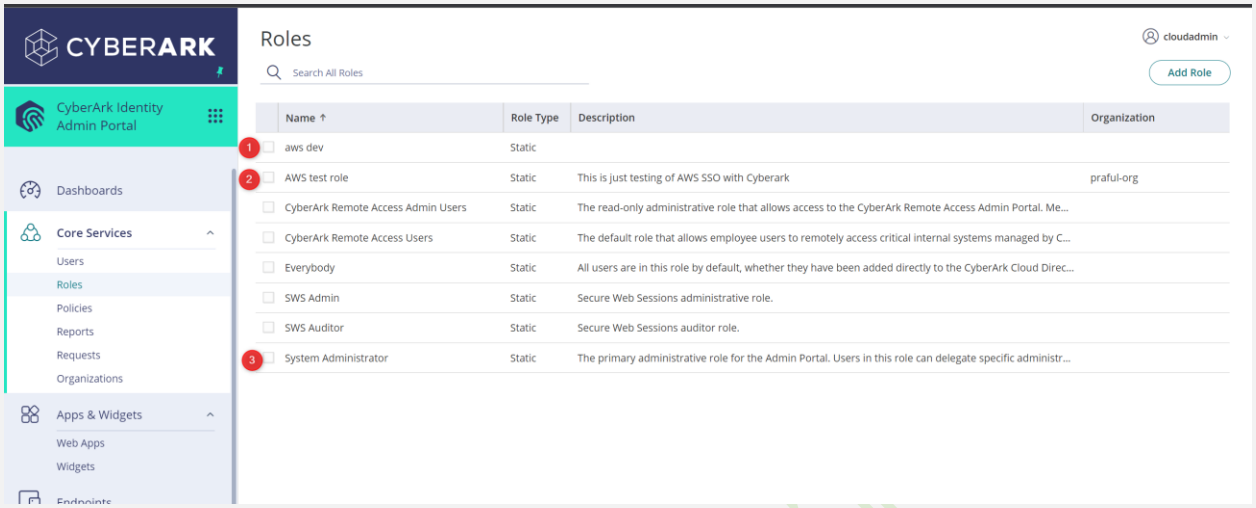


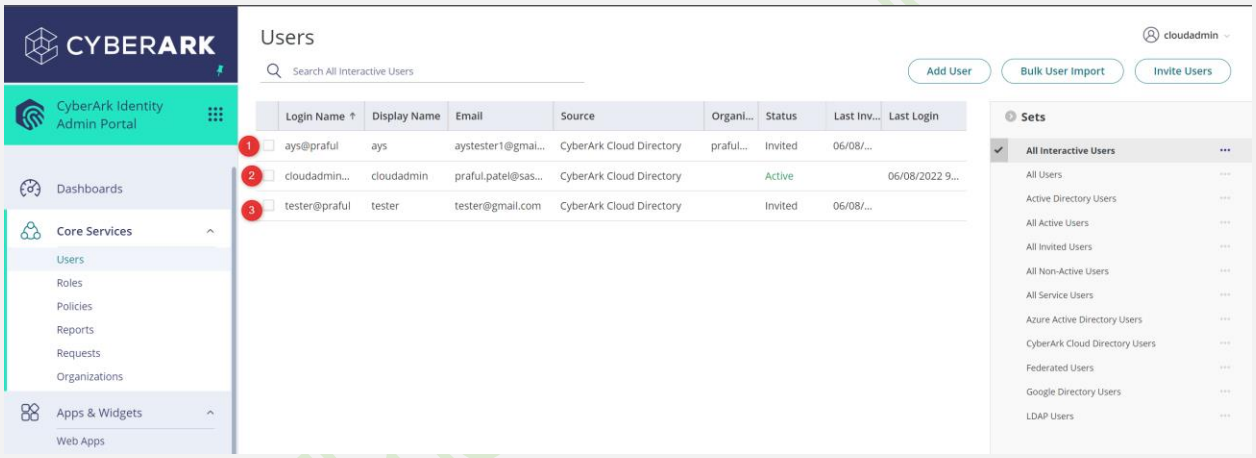



Single Sign-On
Dashboard
AWS accounts
Permission sets
Applications
Users
Groups
Settings
AWS SSO > Groups
Your identity source is currently configured as 'External identity provider'. To add new groups or edit their memberships, you must do this using your external identity provider.
Groups (2)
Delete group
Find groups by group name
Group name
Users
Description
Created by
test admn
1 user
SCIM
aws dev
1 user
SCIM

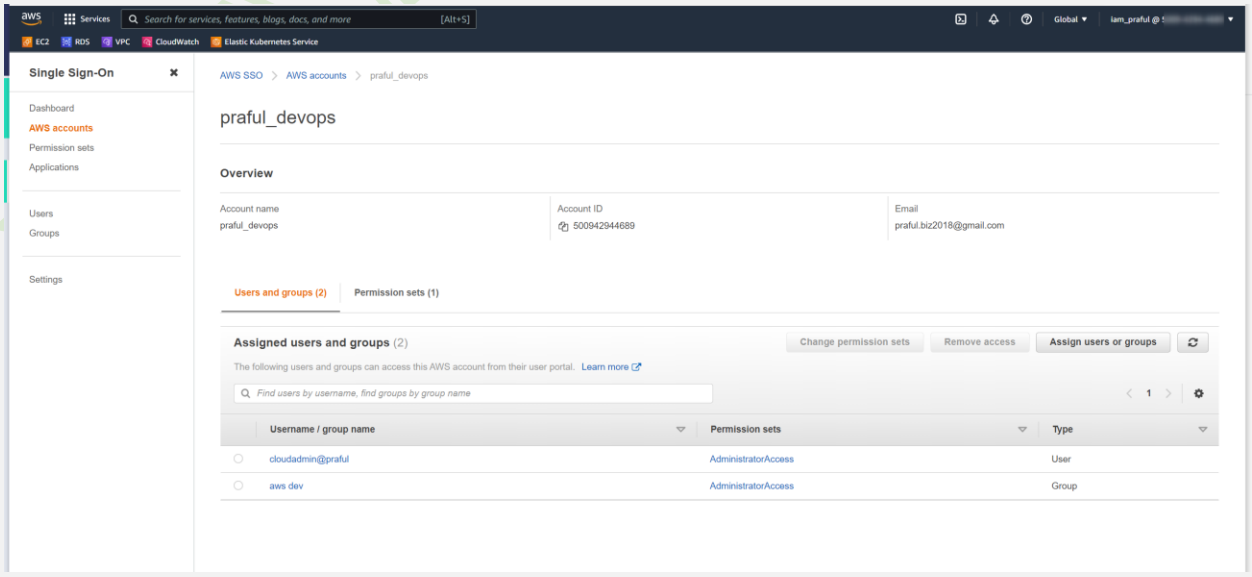

Gmail
Search mail
Compose
Inbox 2,069
Starred
Snoozed
Important
Sent
Drafts
Categories
GoogleDrive
Not An Issue
New meeting
Join a meeting
No recent chats
Start a new one
1 of 757
CyberArk Identity Service - User Account
Inbox
GoogleDrive
CyberArk Account Management @ aan4620.my.idaptive.app <noreply-cloudadmin-praful@aan4620.my.idaptive.app>
to me
3:06 PM (25 minutes ago)
CYBERARK
Welcome to CyberArk Identity!
Congratulations! You've been invited to CyberArk Identity by your system administrator.
Access the User Portal
to start using your applications and services.
Login Now
Here are your account details:
login name: ays@praful
If you need help or have any questions, please contact your system administrator.

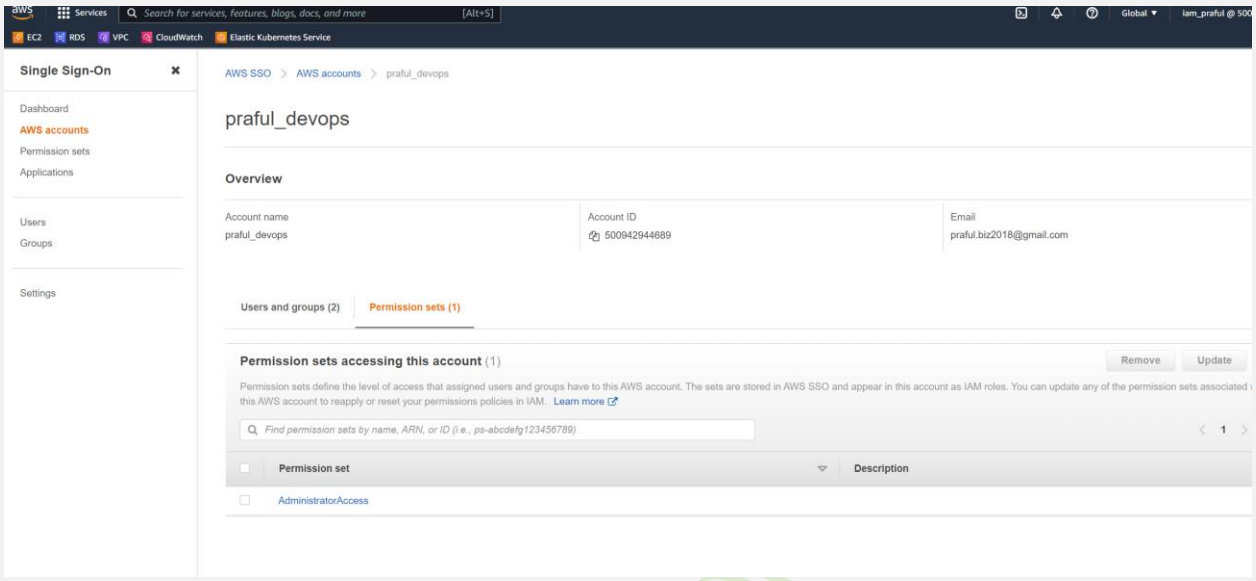

Single Sign-On
Dashboard
AWS accounts
Permission sets
Applications
Users
Groups
Settings
AWS SSO > Users
Your identity source is currently configured as 'External identity provider'. To add new users or edit their attributes, you must do this using your external identity provider.
Users (2)
Users listed here can sign in to the user portal to access any AWS accounts or applications that you have assigned to them.
Username
Find users
Username
Display name
Status
Created by
cloudadmin@praful
cloudadmin
Enabled
SCIM
ays@praful
ays
Enabled
SCIM



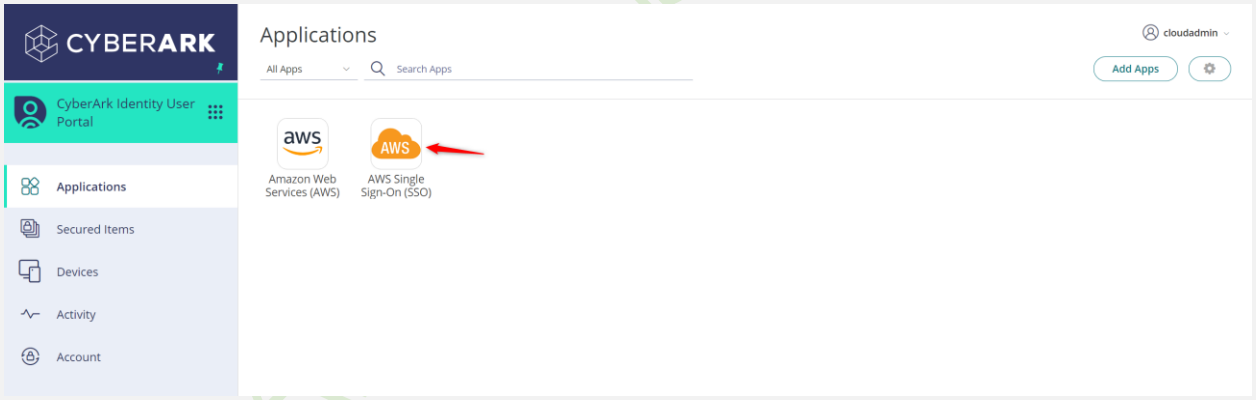


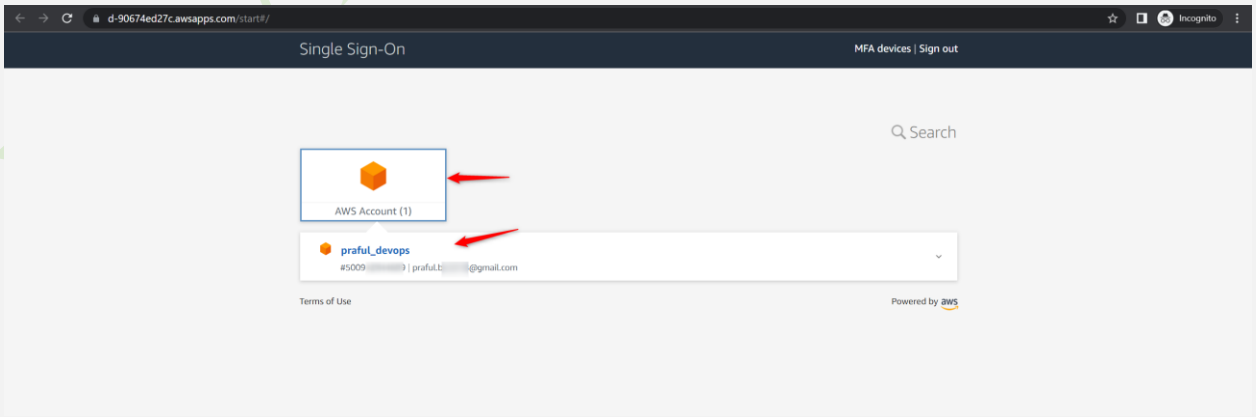
Assign permission to user and group

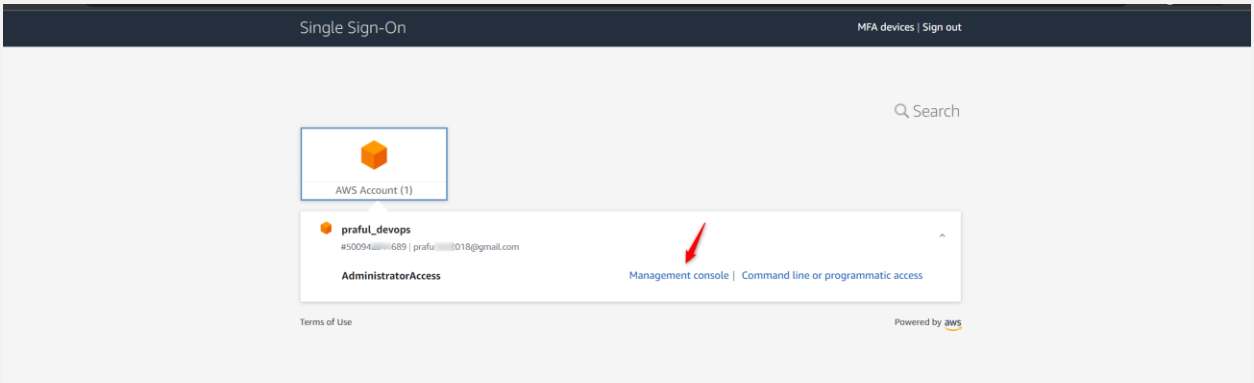




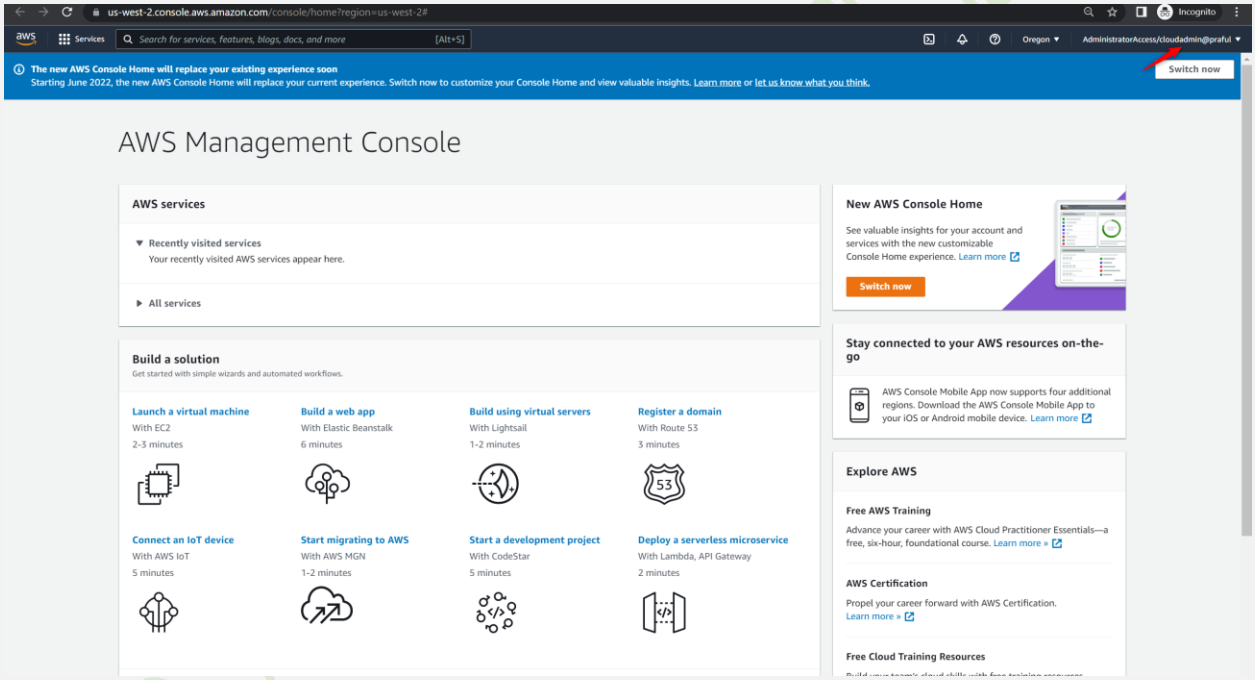
Go to Cyberark user login







User is logged in using cyberark identity in AWS SSO



Reference: https://aws.amazon.com/blogs/apn/federated-access-to-aws-single-sign-on-with-cyberark-workforce-identity/?nc1=b_rp

CHALLENGE

Congratulations!!!!