



<https://linkedin.com/in/prafulpatel16>

<https://github.com/prafulpatel16>

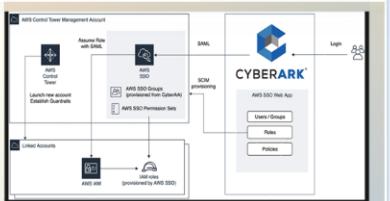
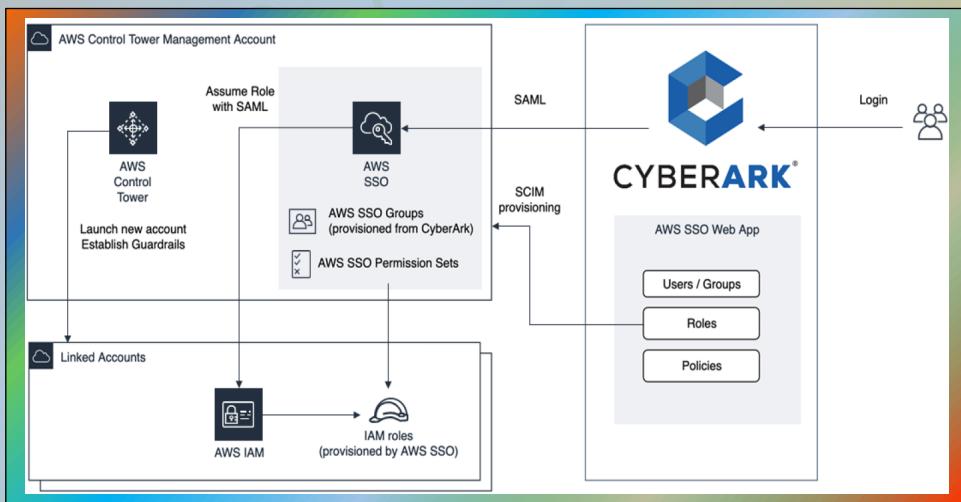


AWS PROJECT

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH CYBERARK

WORKFORCE IDENTITY

IMPLEMENTED BY: PRAFUL PATEL



Date: June 08, 2022

PRAFUL PATEL | CYBERARK

➤ **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 vary based on adding and removing services based on requirement.)

➤ **Pre-requisites:**

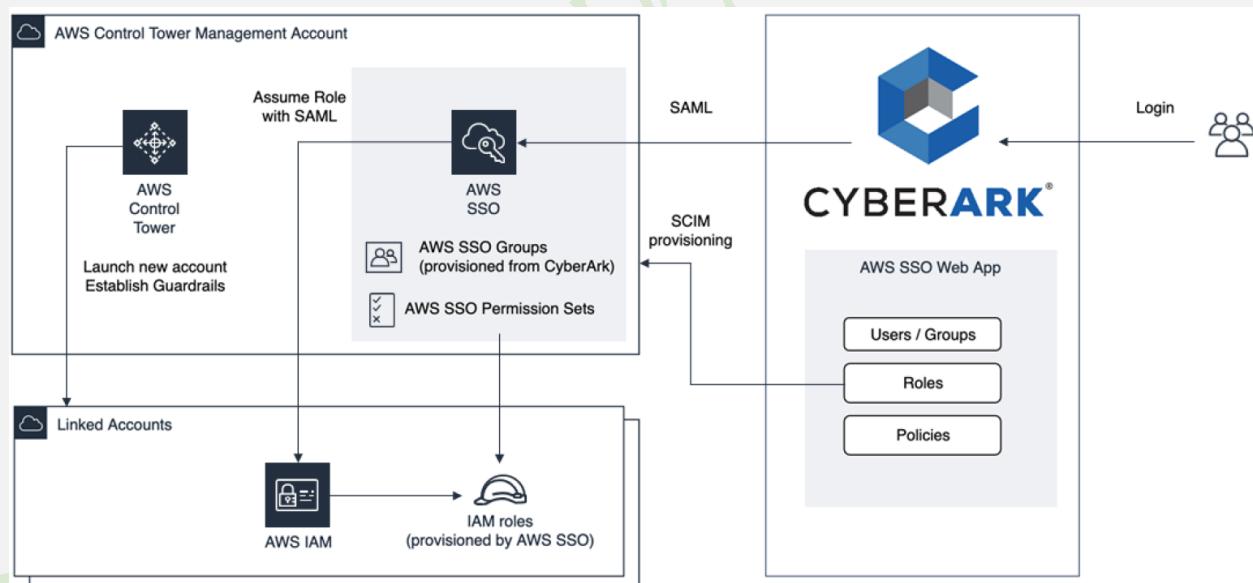
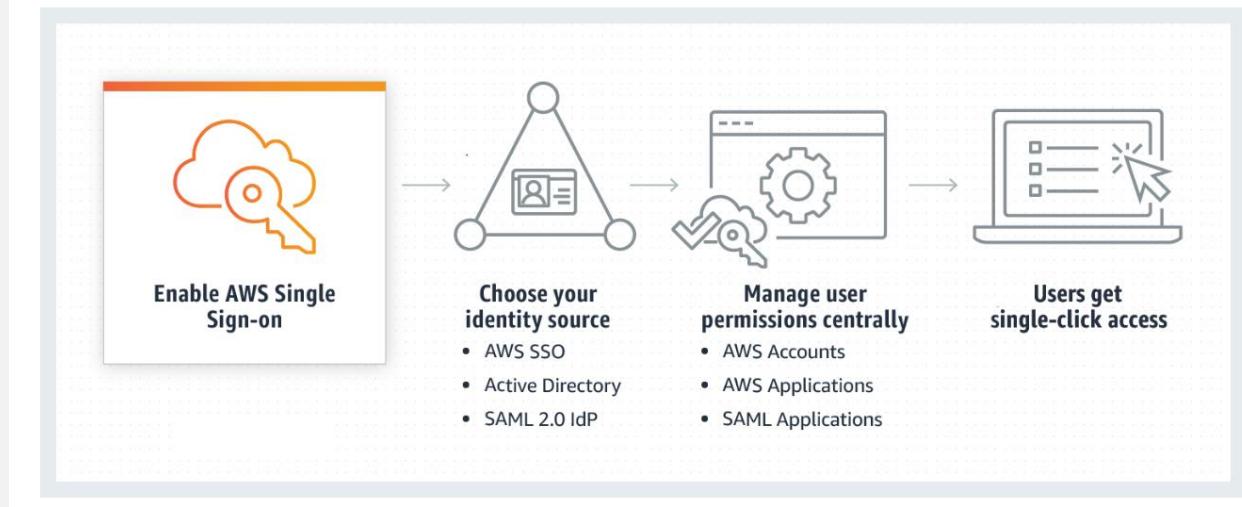
1. AWS SSO enabled- AWS Organization account
2. CyberArk Workforce Identity on AWS Marketplace OR
3. CyberArk Identity free trial sign-up

➤ **Tools & Technologies covered:**

- AWS Single Sign-On(SSO)
- CyberArk Identity provider
- SAML 2.0 Authentication

➤ **Solution Architecture:**

Using AWS SSO to access your accounts and applications



➤ **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

The screenshot shows the CyberArk Identity Admin Portal interface. On the left, there's a sidebar with a navigation menu. The main area is titled "Applications" and lists two items: "CyberArk Identity User Portal" and "Admin Portal". The "Admin Portal" item is highlighted with a green box. The sidebar also includes sections for "Secured Items", "Devices", "Activity", and "Account". At the top right, there are buttons for "Add Apps" and "Settings".

Dashboard

The screenshot shows the CyberArk Identity Admin Portal dashboard. The left sidebar has a "Dashboards" section selected. The main dashboard area has a title "Dashboards" and a subtitle "Security Overview". It features several data visualizations: a bar chart for "Denied Logins and Self Service" (1.0), a map showing locations like Sandra Schmirler Leisure Centre and Windsor Park, and two large circular charts for "MFA Factors" and "Login and Self Service Types", both showing a value of 2. Below these are tables for "Denied Logins" (2), "Denied Feature Access" (0), and "Denied Self Service" (0). A detailed table shows event logs for failed logins on June 8, 2022.

Occurred	User	Event Result
06/08/2022 09:39 AM	cloudadmin	Failed login. Result: Challenge not answered or answered incorr...
06/07/2022 06:40 PM	cloudadmin	Failed login. Result: ForgotPassword successful, restarting MFA

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.

Dashboards

Security Overview ▾

Denied Logins and Self Service 1.0

Denied Logins	Denied Feature Access	Denied Self Service
2	0	0

Details

Occurred	User	Event Result
06/08/2022 09:39 AM	cloudadmin	Failed login. Result: Challenge not answered or answered incorrectly.
06/07/2022 06:40 PM	cloudadmin	Failed login. Result: ForgotPassword successful, restarting MFA

MFA Factors

UP 2

Login and Self Service Types

MFA Login 2

Web Apps

Search All Web Applications

	Name ↑	Type	Description	Provisioning	App Gateway	Status
<input type="checkbox"/>	CyberArk Remote Access Portal	Web - SAML	Re...			Deployed
<input type="checkbox"/>	CyberArk Secure Web Sessions Portal	Web - SAML	Cy...			Deployed
<input type="checkbox"/>	User Portal	Web - Portal	Th...			Deployed

Sets

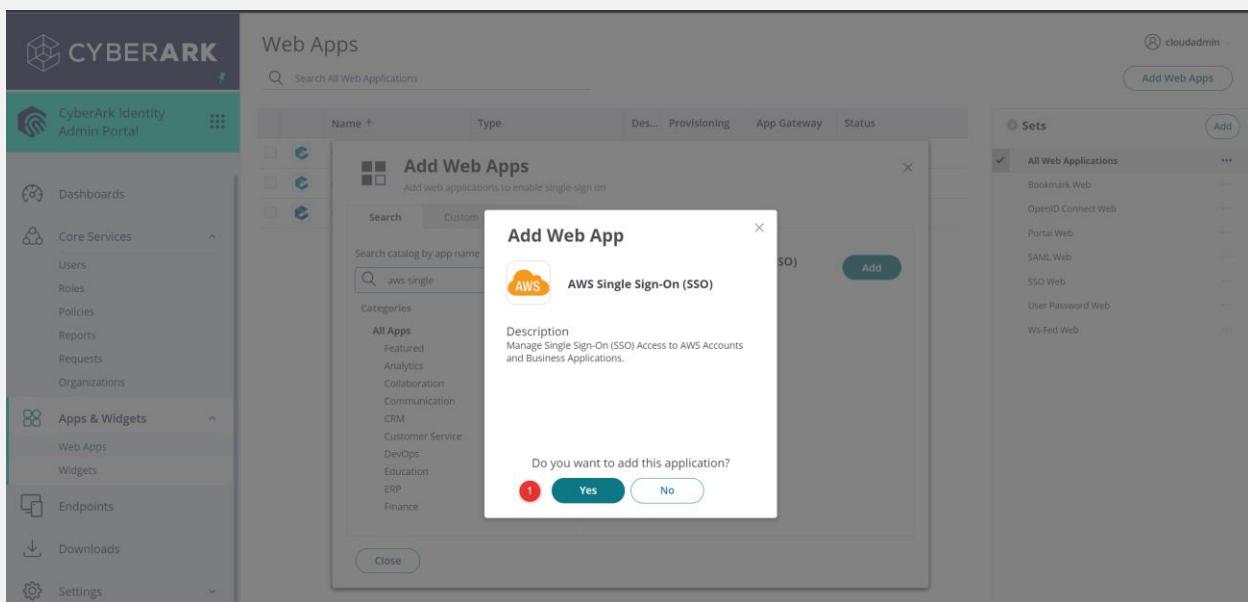
All Web Applications

- Bookmark Web
- OpenID Connect Web
- Portal Web
- SAML Web
- SSO Web
- User Password Web
- Ws-Fed Web

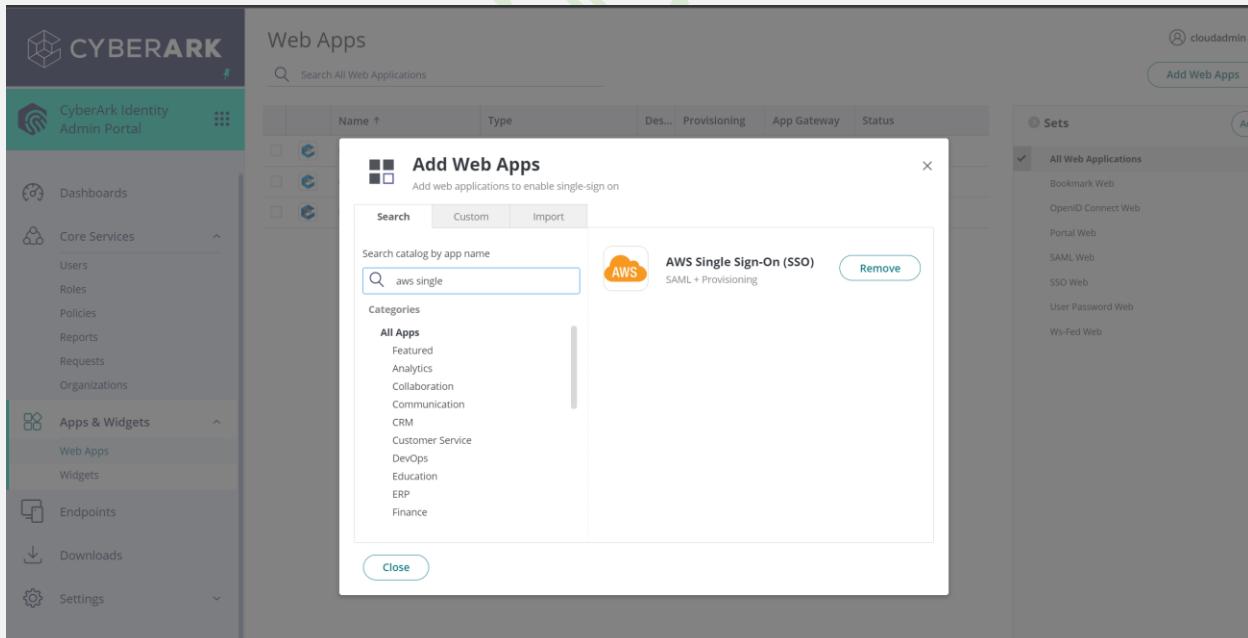
The screenshot shows the CyberArk Identity Admin Portal interface. On the left, there's a sidebar with navigation links like Dashboards, Core Services (Users, Roles, Policies, Reports, Requests, Organizations), Apps & Widgets (Web Apps, Widgets), Endpoints, Downloads, and Settings. The main area is titled 'Web Apps' and contains a table with three rows: 'CyberArk Remote Access ...' (Web - SAML, Re..., Deployed), 'CyberArk Secure Web Ses...' (Web - SAML, Cy..., Deployed), and 'User Portal' (Web - Portal, Th..., Deployed). To the right of the table is a sidebar titled 'Sets' with a list of 'All Web Applications' including 'Bookmark Web', 'OpenID Connect Web', 'Portal Web', 'SAML Web', 'SSO Web', 'User Password Web', and 'Ws-Fed Web'. At the top right of the main content area, there's a button labeled 'Add Web Apps' with a red arrow pointing to it.

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

This screenshot shows the 'Add Web Apps' dialog box overlaid on the CyberArk Identity Admin Portal. The dialog has a search bar with 'aws Single Sign-On' typed into it (marked with a red circle 1). Below the search bar, there's a section for 'AWS Single Sign-On (SSO)' with the subtext 'SAML + Provisioning'. To the right of this section is a green 'Add' button with a red circle 2. The background of the dialog shows a list of categories: All Apps, Featured, Analytics, Collaboration, Communication, CRM, Customer Service, DevOps, Education, ERP, and Finance. At the bottom of the dialog are 'Close' and 'Cancel' buttons.



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.



AWS PROJECT CYBERARK WORKFORCE IDENTITY

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH
IMPLEMENTED
BY: PRAFUL PATEL

The screenshot shows the CyberArk Identity Admin Portal interface. On the left, there's a navigation sidebar with sections like Dashboards, Core Services (Users, Roles, Policies, Reports, Requests, Organizations), Apps & Widgets (Web Apps selected), Endpoints, Downloads, and Settings. The main area is titled 'Web Apps' and contains a table with columns: Name, Type, Description, Provisioning, App Gateway, and Status. One row for 'AWS Single Sign-On (SSO)' is highlighted with a red border. To the right, there's a sidebar for 'Sets' containing a list of pre-defined sets for web applications.

This screenshot shows the configuration details for the 'AWS Single Sign-On (SSO)' application. The left sidebar is identical to the previous screenshot. The main content area shows the application's type as 'Web - SAML + Provisioning' and its status as 'Ready to Deploy'. It includes tabs for 'Settings' (selected), 'Trust', 'SAML Response', 'Permissions', 'Policy', 'Account Mapping', 'Linked Applications', 'Provisioning', 'Workflow', 'Changelog', 'Secure Web Sessions', and 'Widgets'. Under 'Settings', there are fields for 'Name' (AWS Single Sign-On (SSO)), 'Description' (Manage Single Sign-On (SSO) Access to AWS Accounts and Business Applications), 'Category' (DevOps), and a 'Logo' section with a placeholder for an AWS logo. Below these are 'Advanced' settings for 'Application ID' and 'App Key', with a 'Copy Key' button. At the bottom are 'Save' and 'Cancel' buttons.

- 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.

CYBERARK

CyberArk Identity Admin Portal

Back to Web Apps | 1 of 4 | cloudadmin | Actions

Type: Web - SAML + Provisioning | Status: Ready to Deploy | Application Configuration Help | Actions

Trust

Identity Provider Configuration

Configure your IdP Entity ID / IdP Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values in a certain method. Choose the method, then follow the instructions.

Metadata

Manual Configuration

Metadata

IdP Entity ID / IdP Issuer

https://aan4620.my.idaptive.app/cbe7345b-0ff-... | Copy (1)

Signing Certificate

AAN4620 SHA256 Application Signing Certificate (default) | 2

Thumbprint: A6A9B5F70BE8F87B39EC9D...
Subject: CN=AAN4620 Application Signing Certificate
Algorithm: sha256RSA
Expires: 12/31/2038 6:00:00 PM

Download (3)

Single Sign On URL

https://aan4620.my.idaptive.app/run?... | Copy (4)

URL: https://aan4620.my.idaptive.ap... | Copy URL

File: Download Metadata File

XML: Copy XML

Save | Cancel

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

CYBERARK

CyberArk Identity Admin Portal

Back to Web Apps | 1 of 4 | cloudadmin | Actions

Type: Web - SAML + Provisioning | Status: Ready to Deploy | Application Configuration Help | Actions

Trust

Identity Provider Configuration

Configure your IdP Entity ID / IdP Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values in a certain method. Choose the method, then follow the instructions.

Metadata

Manual Configuration

Metadata

IdP Entity ID / IdP Issuer

https://aan4620.my.idaptive.app/cbe7345b-0ff-... | Copy

Signing Certificate

AAN4620 SHA256 Application Signing Certificate (default)

Thumbprint: A6A9B5F70BE8F87B39EC9D...
Subject: CN=AAN4620 Application Signing Certificate
Algorithm: sha256RSA
Expires: 12/31/2038 6:00:00 PM

Download

Single Sign On URL

https://aan4620.my.idaptive.app/run?... | Copy

URL: https://aan4620.my.idaptive.ap... | Copy URL

File: Download Metadata File

XML: Copy XML

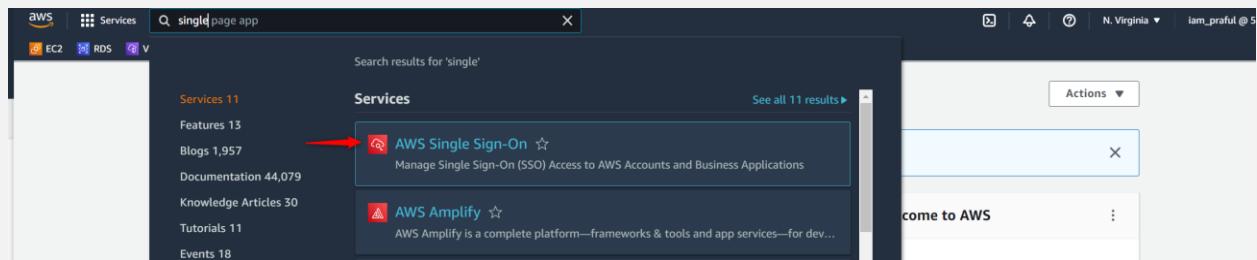
Save | Cancel

AAN4620 SHA256.cer

6. 7. Configuring New External Identity Provider

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

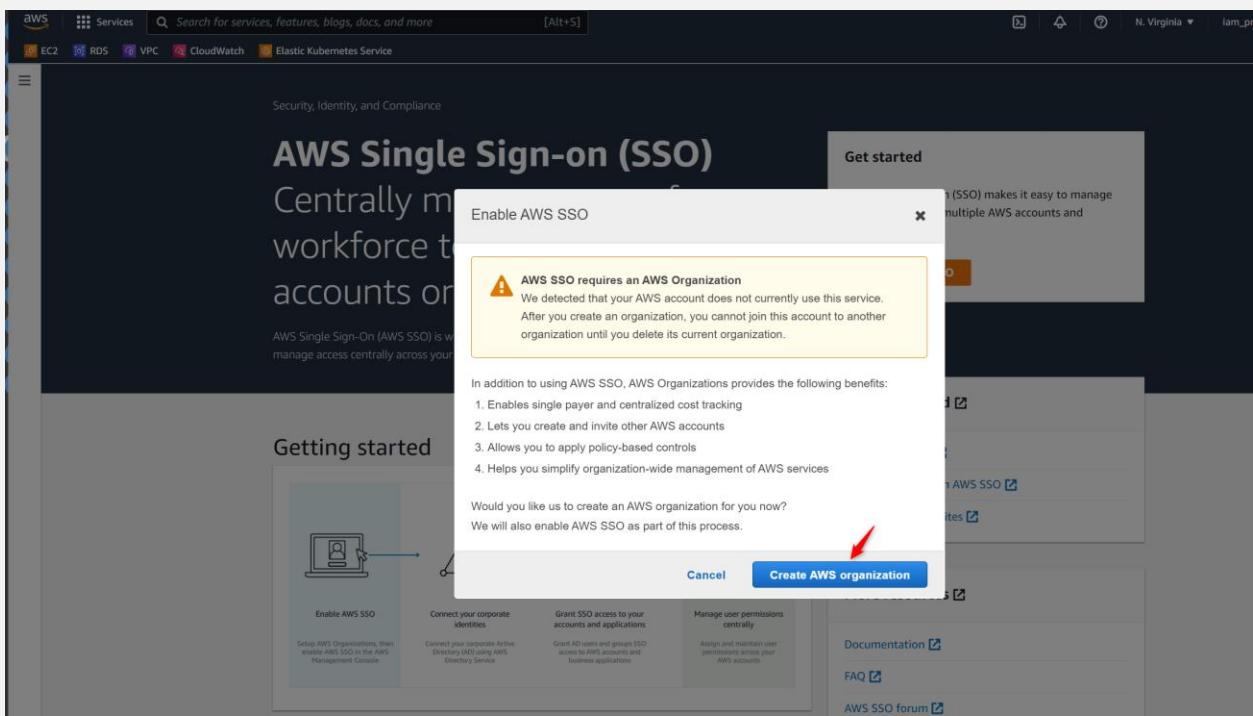
BY: PRAFUL PATEL



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

The screenshot shows the AWS Single Sign-on (SSO) landing page. It features a large title 'AWS Single Sign-on (SSO)' and a subtitle 'Centrally manage access for your workforce to multiple AWS accounts or applications.' A 'Get started' section on the right contains a 'Enable AWS SSO' button, which is highlighted with a red arrow. Below the main title is a 'Getting started' diagram illustrating the four steps: Enable AWS SSO, Connect your corporate identities, Grant SSO access to your accounts and applications, and Manage user permissions centrally.

Create Organization



Click on Actions

Click change identity source

Screenshot of the AWS Single Sign-On Settings page under the 'Identity source' tab. The page shows basic configuration details like ARN, Region, and AWS SSO as the identity source. A prominent red arrow points to the 'Change identity source' button in the top right corner of the main content area.

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

Screenshot of the 'Change identity source' wizard, Step 1: Choose identity source. The page lists three options: AWS SSO, Active Directory, and External identity provider. The 'External identity provider' option is selected and highlighted with a blue circle. A red arrow points to the 'Next' button at the bottom right of the form.

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:

Step 1
Choose identity source

Step 2
Configure external identity provider

Step 3
Confirm change

Service provider metadata

1 AWS SSO Sign-in URL
https://d-90674ed2...
2 AWS SSO ACS URL
https://us-east-1.siginin.aws.amazon.c...
3 AWS SSO issuer URL
https://us-east-1.siginin.a...

Identity provider metadata

Depending on the identity provider, you may have to:

IdP SAML metadata
Choose file

Or

IdP sign-in URL

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:

CYBERARK

CyberArk Identity Admin Portal

Back to Web Apps

AWS Single Sign-On (SSO)

Type: Web - SAML + Provisioning Status: Ready to Deploy

Trust

Identity Provider Configuration

Configure your IdP Entity ID / IdP Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values in a certain method. Choose the method, then follow the instructions.

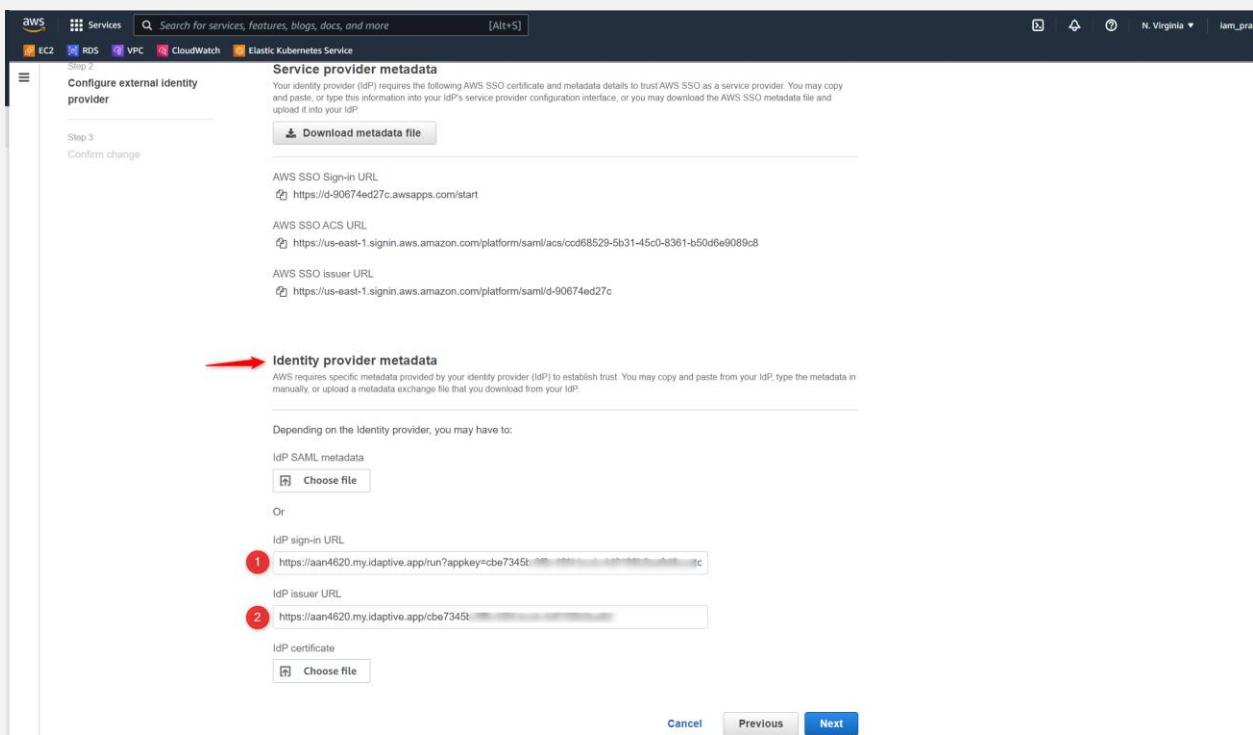
Metadata

IdP Entity ID / IdP Issuer
https://aan4620.my.idaptive.app/cbe7...
Copy

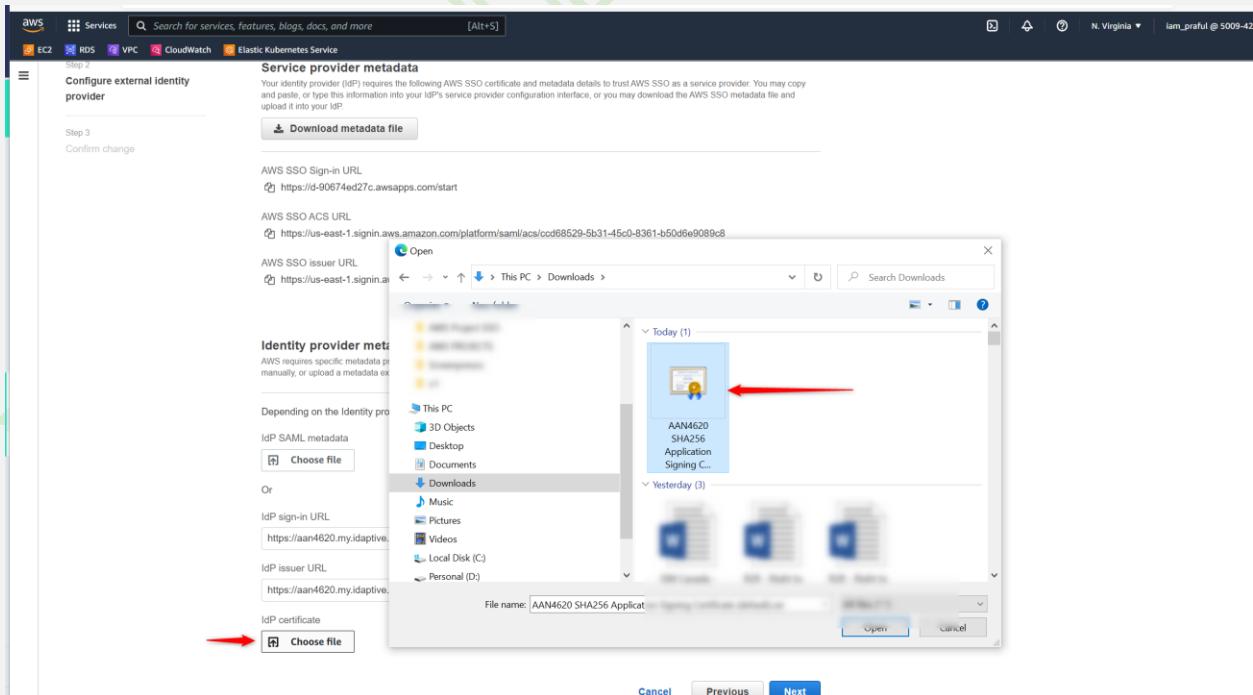
Signed Certificate
AAAN4620.SIAQZ6 Application Signing Certificate (default)
Download

Single Sign On URL
https://aan4620.my.idaptive.app/run?appk...
Copy

URL: https://aan4620.my.idaptive.app/saasManage/Downl...
File: Download Metadata File



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



Certificate upload successful

AWS PROJECT CYBERARK WORKFORCE IDENTITY

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH IMPLEMENTED BY: PRAFUL PATEL

Step 3
Confirm change

Download metadata file

AWS SSO Sign-in URL
https://d-90674ed27c.awssapps.com/start

AWS SSO ACS URL
https://us-east-1.sigin.aws.amazon.com/platform/saml/acs/ccd68529-5b31-45c0-8361-b50d6e9089cb

AWS SSO issuer URL
https://us-east-1.sigin.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

Or

IdP sign-in URL
https://aan4620.my.idaptive.app/run?appid=...&...&...&...&...&...&...

IdP issuer URL
https://aan4620.my.idaptive.app/cbe734f1-08b-4561-9...&...

IdP certificate

AAN4620 SHA256 Application Signing Certificate (default).cer
Size: 1324 bytes
Last modified: Jun 8, 2022

Cancel **Previous** **Next**

Step 1
Choose identity source

Step 2
Configure external identity provider

Step 3
Confirm change

Download metadata file

1 AWS SSO Sign-in URL
https://d-90674ed27c.awssapps.com/start

2 AWS SSO ACS URL
https://us-east-1.sigin.aws.amazon.com/...

3 AWS SSO issuer URL
https://us-east-1.sigin.aws.amazon.com/...

Service provider metadata
Your identity provider (IdP) requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.

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

Or

IdP sign-in URL
https://aan4620.my.idaptive.app/run...
4

IdP issuer URL
https://aan4620.my.idaptive.ap...
5

IdP certificate

AAN4620 SHA256 Application Signing Certificate (default).cer
Size: 1324 bytes
Last modified: Jun 8, 2022

Cancel **Previous** **Next**

BY: PRAFUL PATEL

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

Step 2: Configure external identity provider

Service provider metadata

IdP certificate AAN4620 SHA256 Application Signing Certificate (default).cer Size: 1124 bytes Last modified: Jun 8, 2022	IdP sign-in URL: https://iam4620.my.adaptiveapprun.apigkey 4d0152 0	IdP issuer URL: https://ai... 345b-off
---	--	--

Review and confirm

⚠ Review the following consequences of your requested identity source change:

- You are changing your identity source to use an external identity provider (IdP).
- AWS SSO will delete your existing multi-factor authentication (MFA) configuration.
- All existing permission sets and SAML application configurations will be retained.
- AWS SSO preserves your existing users, groups, and their assignments. However, only users with matching usernames in your IdP can authenticate.
- You must complete your IdP SAML configuration to AWS SSO in order for your users to be able to sign in to AWS SSO using your IdP for a successful authentication.
- You must enable multi-factor authentication (MFA) configuration and policies in your IdP.
- You must add (provision) all your IdP users who will use AWS SSO before they can sign in. If you enable SCIM to provision users and groups (recommended), your IdP will be the authoritative source of users and groups, and you must add and modify all users and groups in your IdP. Without SCIM, you provision users and manage groups in AWS SSO only; all provisioned usernames must match corresponding IdP usernames.
- AWS SSO will keep your current configuration of attributes for access control. You should review your configuration and update after completing the identity source change.

Confirm that you want to change your identity source by entering ACCEPT in the field below.

ACCEPT 1 2 **Previous** **Change identity source**

Single Sign-On

Settings

Details

Configure your identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and cloud applications.

ARN 1 arn:aws:sso-instance:soicons

Region US East (N. Virginia) | us-east-1

Delegated administrator AWS SSO-integrated applications 2 Enabled in member accounts

Attributes for access control

Configure this option when you need to federate access to your users and groups based on key-value pairs you identify for a specific incoming attribute. [Learn more](#) ? **Enable**

Automatic provisioning

When your identity source is set to External identity provider, you can configure how best to provision all your users and groups into AWS SSO so that you can make assignments to the AWS accounts or applications you have configured. [Learn more](#) ? **Enable**

Identity source

Determine where you administer your users and groups, and where AWS SSO authenticates your users. [Learn more](#) ?

Identity source 3

Authentication method SAML 2.0 4

User portal URL 5 https://id-9067.iam.awsapps.com/start

Provisioning method Manual

Identity store ID 6 d-9067

Actions 7

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.

The screenshot shows the CyberArk Identity Admin Portal interface. On the left, there is a navigation sidebar with sections like Dashboards, Core Services, Apps & Widgets, Endpoints, Downloads, and Settings. The 'Trust' section is highlighted with a red circle containing the number 1. In the main content area, the title is 'AWS Single Sign-On (SSO)' with a status of 'Ready to Deploy'. The 'Type' is listed as 'Web - SAML + Provisioning'. The 'Trust' tab is selected, showing the 'Manual Configuration' form. A red circle containing the number 2 points to the 'Manual Configuration' radio button. A red circle containing the number 3 points to the 'SP Entity ID / SP Issuer / Audience' field, which contains the value 'https://signin.aws.amazon.com/platform/saml'. Below this, the 'Assertion Consumer Service (ACS) URL' field is populated with 'https://signin.aws.amazon.com/platform/saml'. Other fields include 'Recipient' (set to 'Same as ACS URL'), 'NameID Format' (set to 'emailAddress'), and 'Authentication Context Class' (set to 'unspecified'). At the bottom, there are 'Save' and 'Cancel' buttons.

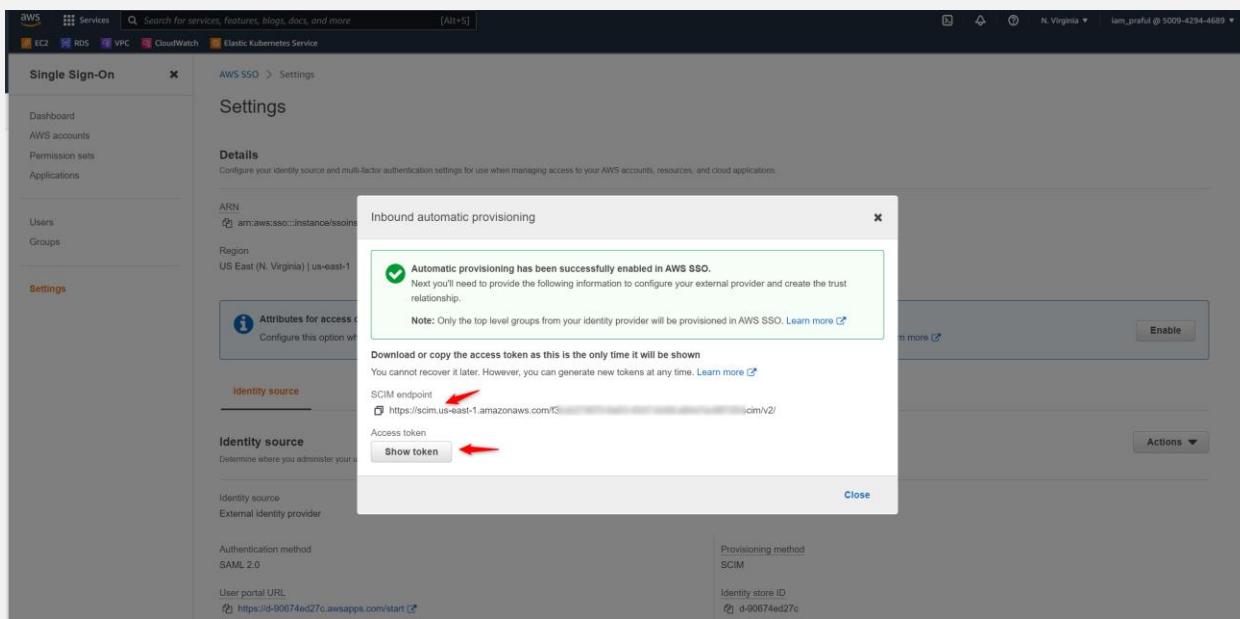
2. Paste the AWS SSO issuer URL you copied from AWS SSO in the SP Entity ID/ SP Issuer/Audience field
3. Paste the AWS SSO CS URL you copied from AWS SSO in the Assertion Consumer Service (ACS) URL field.
4. The Recipient field should be the same as the ACS URL.
5. Make sure the NameID Format is set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

BY: PRAFUL PATEL

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.

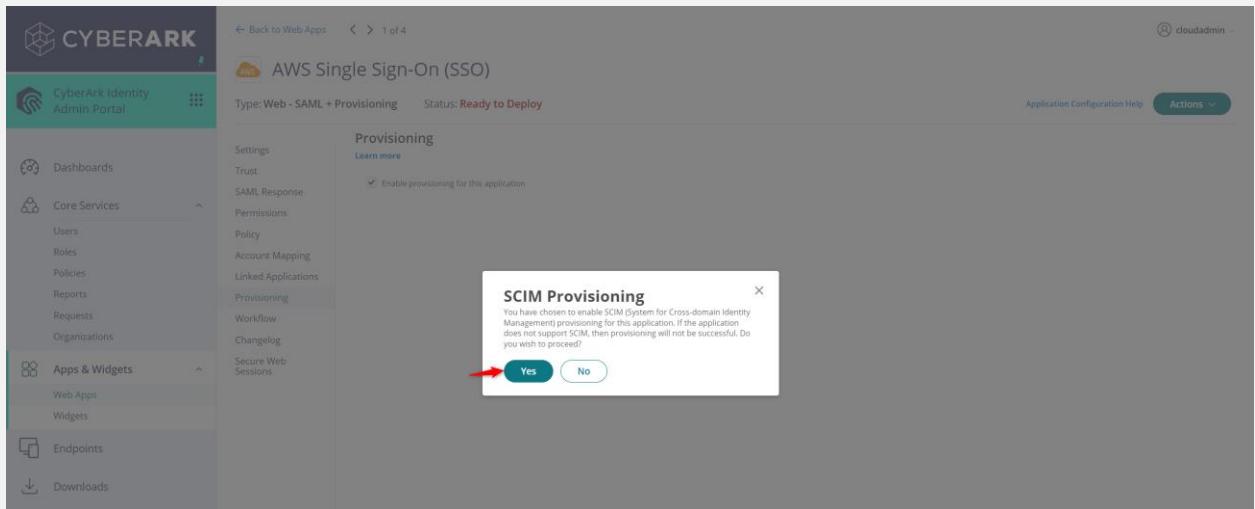


CyberArk Workforce Identity – Configuring SCIM

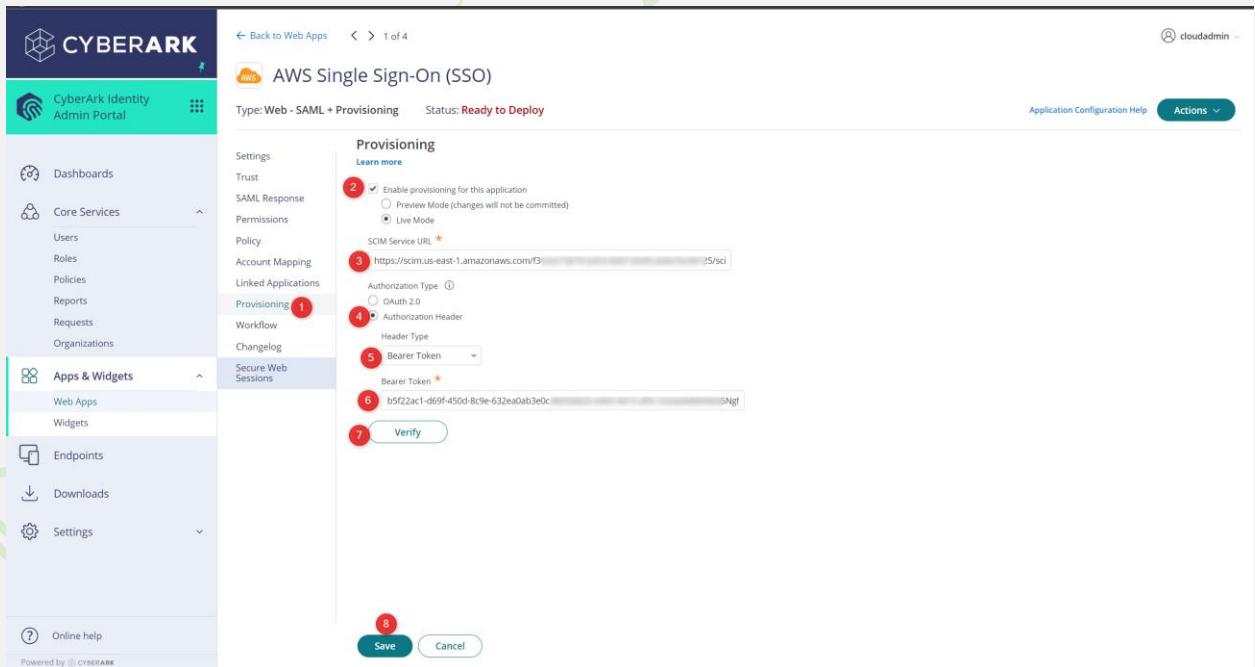
1. Return to the CyberArk Workforce Identity admin portal. Go to the Provisioning tab and check the box to Enable Provisioning for this application.

The screenshot shows the CyberArk Identity Admin Portal interface. On the left, there's a sidebar with navigation links like Dashboards, Core Services (Users, Roles, Policies, Reports, Requests, Organizations), Apps & Widgets (Web Apps, Widgets), Endpoints, Downloads, and Settings. The main content area is titled 'AWS Single Sign-On (SSO)' and shows it's a 'Web - SAML + Provisioning' type application with a status of 'Ready to Deploy'. Under the 'Provisioning' section, there's a checkbox labeled 'Enable provisioning for this application' which is checked. A red arrow points to this checkbox. Other options in the Provisioning menu include Learn more, Settings, Trust, SAML Response, Permissions, Policy, Account Mapping, Linked Applications, Workflow, Changelog, and Secure Web Sessions. At the top right, there are 'Application Configuration Help' and 'Actions' buttons.

BY: PRAFUL PATEL



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.

AWS PROJECT CYBERARK WORKFORCE IDENTITY

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH IMPLEMENTED

BY: PRAFUL PATEL

Provisioning

Bearer Token: b5f22ac1-d6f9-450d-8c9e-632e...

Sync Options:

- 1 Sync (overwrite) users to target application when existing users are found with the same principal name.
- 2 Do not sync (no override) users to target application when existing users are found with the same principal name.
- 3 Do not de-provision (deactivate or delete) users in target application when the users are removed from mapped role.
- 4 Sync groups from local directory to target application. This option overrides any destination group selection in Role Mappings.
- 5 User De-provisioning Options:
 - Disable user
 - Delete user

Role Mappings

Add

Name: Nothing configured

Provisioning Script

Save Cancel

Add Role: AWS Role

Role Mapping

Select the Role and (0) Destination Groups to create a role mapping. For best results, mappings should not include users that are in more than one mapped role.

Role: CyberArk Remote Access Admin Users

Destination Group:

- Add (highlighted by a red arrow)
- AWS Role (highlighted by a red arrow)

Done Cancel

Go to Settings

Users

BY: PRAFUL PATEL

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.

AWS Single Sign-On (SSO)

Type: Web - SAML + Provisioning Status: Ready to Deploy

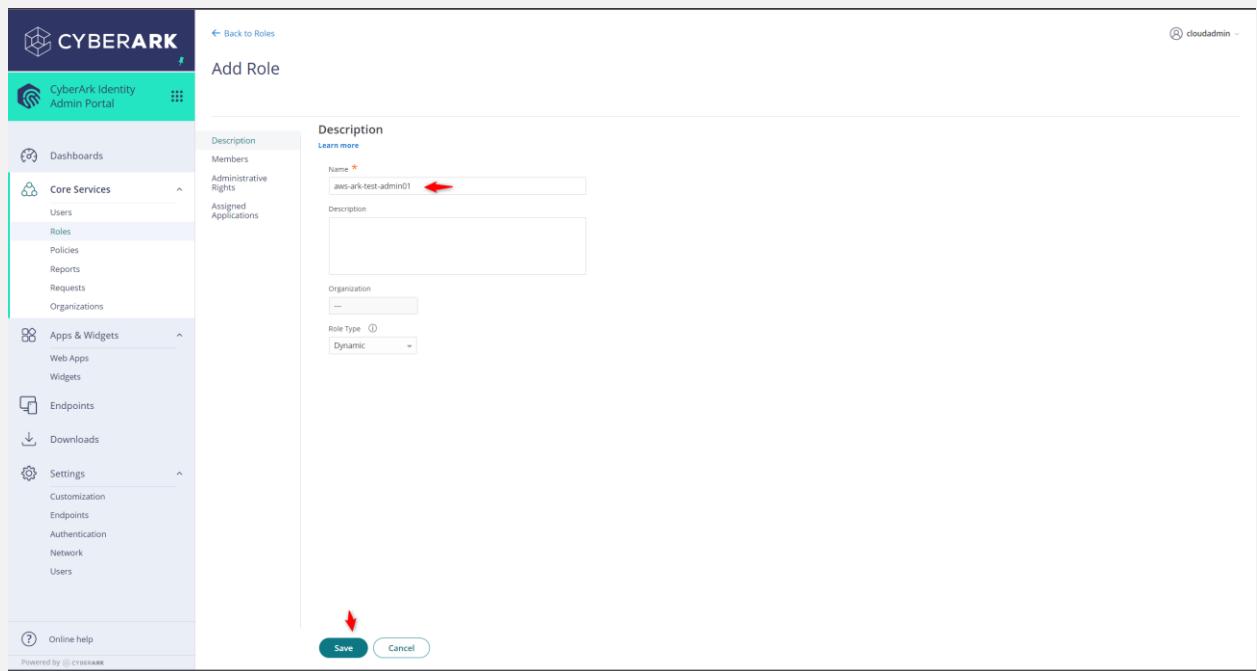
Permissions

Name	Grant	View	Manage	Delete	Run	Automatically D...	Starts	Expires	Inherited From
aero-integration-user\$@...	✓	✓	✓	✓	□	□	□		Administrative Right: Cy...
sns-integration-user\$@...	✓	✓	✓	✓	□	□	□		Administrative Right: Cy...
System Administrator	✓	✓	✓	✓	□	□	□		Sysadmin

Create a new role

Roles

Name	Role Type	Description	Organization
CyberArk Remote Access ...	Static	The read-only administrative role that allows access to the CyberArk Remote Access Admin Portal. Members of this role are managed directly in CyberArk Remote Acces...	
CyberArk Remote Access ...	Static	The default role that allows employee users to remotely access critical internal systems managed by CyberArk.	
Everybody	Static	All users are in this role by default, whether they have been added directly to the CyberArk Cloud Directory, or are in an external directory connected through a CyberAr...	
SWS Admin	Static	Secure Web Sessions administrative role.	
SWS Auditor	Static	Secure Web Sessions auditor role.	
System Administrator	Static	The primary administrative role for the Admin Portal. Users in this role can delegate specific administrative rights to other roles who require more limited administrative...	



CYBERARK

Add Role

Description

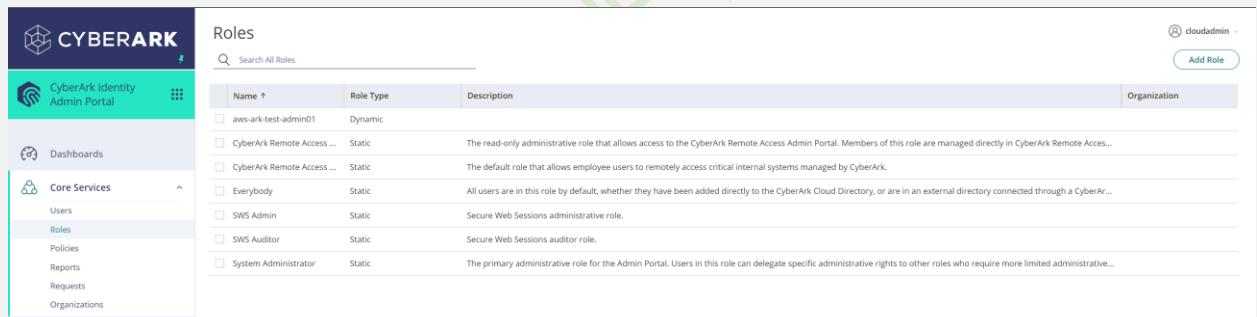
Name * (highlighted)

Description

Organization

Role Type (highlighted)

Save **Cancel**



CYBERARK

Roles

Search All Roles

Name	Role Type	Description	Organization
aws-ark-test-admin01	Dynamic	The read-only administrative role that allows access to the CyberArk Remote Access Admin Portal. Members of this role are managed directly in CyberArk Access...	
CyberArk Remote Access ...	Static	The default role that allows employee users to remotely access critical internal systems managed by CyberArk.	
CyberArk Remote Access ...	Static	The default role that allows employee users to remotely access critical internal systems managed by CyberArk.	
Everybody	Static	All users are in this role by default, whether they have been added directly to the CyberArk Cloud Directory, or are in an external directory connected through a CyberA...	
SWS Admin	Static	Secure Web Sessions administrative role.	
SWS Auditor	Static	Secure Web Sessions auditor role.	
System Administrator	Static	The primary administrative role for the Admin Portal. Users in this role can delegate specific administrative rights to other roles who require more limited administrative...	

Add Role

Add role to AWS SSO

BY: PRAFUL PATEL

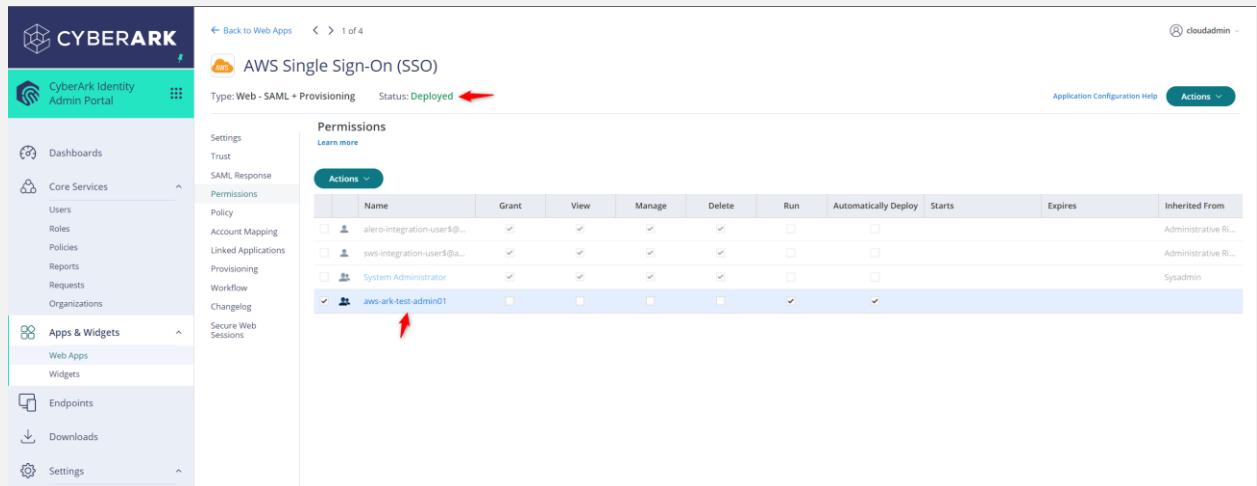
The screenshot shows the CyberArk Identity Admin Portal interface. The left sidebar has sections like Dashboards, Core Services, Apps & Widgets (with 'Web Apps' highlighted by a red circle), Endpoints, Downloads, and Settings. The main area shows a 'AWS Single Sign-On (SSO)' configuration page for a 'Web - SAML + Provisioning' application. A modal window titled 'Select User, Group, or Role' is open, showing a search result for 'aws'. The user 'aws-ark-test-admin01' is selected and highlighted by a red circle. The 'Add' button at the bottom of the modal is also highlighted by a red circle.

The screenshot shows the same CyberArk Identity Admin Portal interface. The 'Permissions' table now includes the user 'aws-ark-test-admin01' under the 'Name' column. A red arrow points to this new row. The 'Actions' dropdown and 'Save' button are also highlighted by red circles.

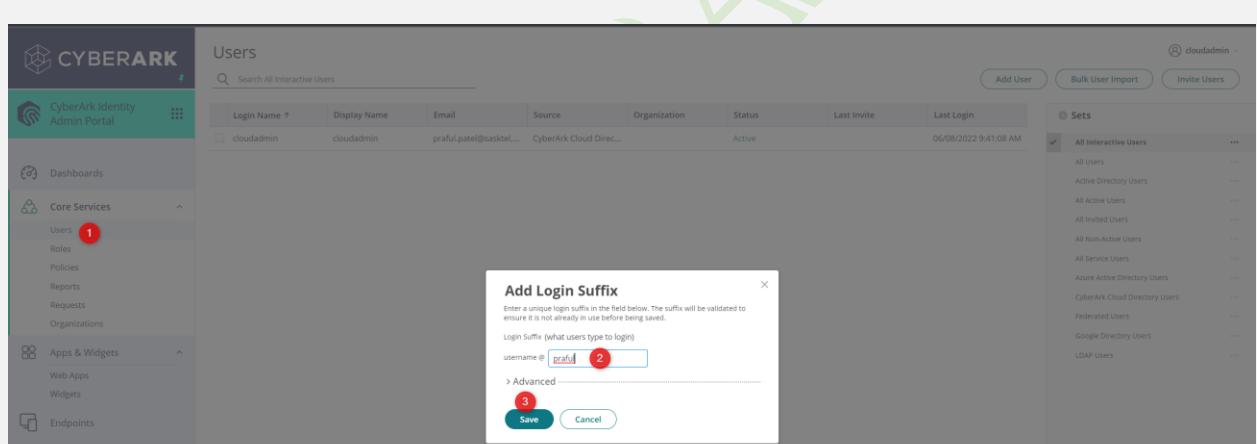
13. Once this step is completed you'll see the status change from Ready to Deploy to Deployed

AWS PROJECT
CYBERARK WORKFORCE IDENTITY

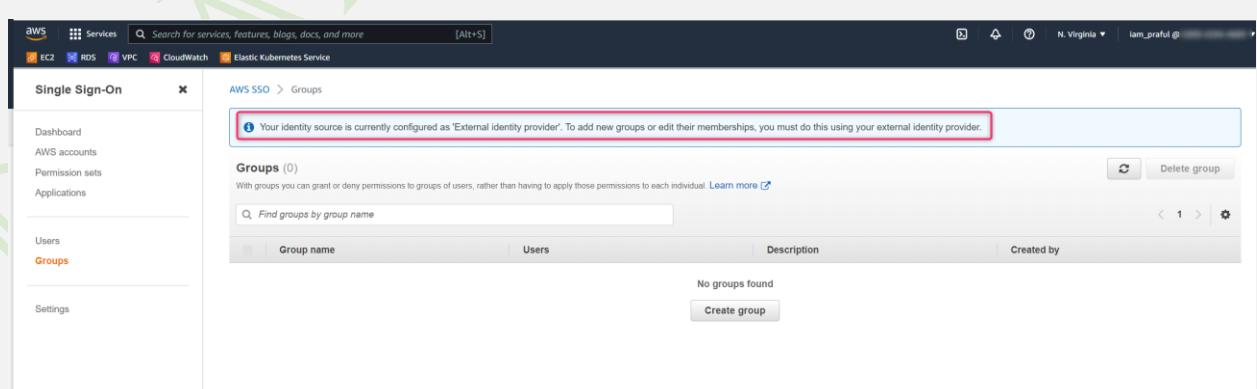
FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH
IMPLEMENTED
BY: PRAFUL PATEL



The screenshot shows the CyberArk Identity Admin Portal interface. On the left, the navigation menu includes Dashboards, Core Services (with Users selected), Apps & Widgets (with Web Apps selected), Endpoints, Downloads, and Settings. The main content area is titled "AWS Single Sign-On (SSO)" and shows the status as "Deployed". A red arrow points to the "Status: Deployed" link. Below this, there is a "Permissions" section with a table showing various users and their permissions. Another red arrow points to the "aws-ark-test-admin01" user row.



This screenshot shows the "Users" page in the CyberArk Identity Admin Portal. The "Users" section in the navigation has a red circle with the number "1" above it. The main table lists a single user: "clouadmin" (Display Name: praful.patel@sasktel...). A red arrow points to the "clouadmin" row. To the right, there is a "Sets" sidebar with various user sets listed. A modal window titled "Add Login Suffix" is open, showing a "username @" input field with "praful" typed in, a "Save" button with a red circle containing the number "2", and a "Cancel" button.



This screenshot shows the AWS Single Sign-On Groups configuration page. The navigation bar includes "AWS SSO" and "Groups". A red box highlights a message: "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." The main table is empty, showing "No groups found" and a "Create group" button. The left sidebar shows "Groups" selected under "Users".

AWS Single Sign-On (SSO)

Type: Web - SAML + Provisioning Status: Deployed

Provisioning

Name	Destination Group
AWS test role	AWS Role, Cloud Admin
System Administrator	test admin

Save Cancel

Click on Sync

Outbound Provisioning

Use these settings to configure application provisioning, where CyberArk identity automatically adds and removes user accounts in web applications.

Sources

Administrative Accounts

Other

Idle User Session Timeout

Reporting options (note: a report is always sent if an error is encountered during sync)

- Send report on full sync
- Send report on individual user sync
- Include debug trace in the report

Synchronization

Select the provisioned application and click the Start Sync button to begin synchronization. A summary report is mailed to the report delivery address on job completion. Note: no account changes are committed for applications in preview mode.

Provisioning Enabled Applications

All Enabled Applications **Start Sync**

View Synchronization Job Status and Reports

Run synchronization daily for all enabled applications

Sync Start Time (UTC / local time)

1 2 3

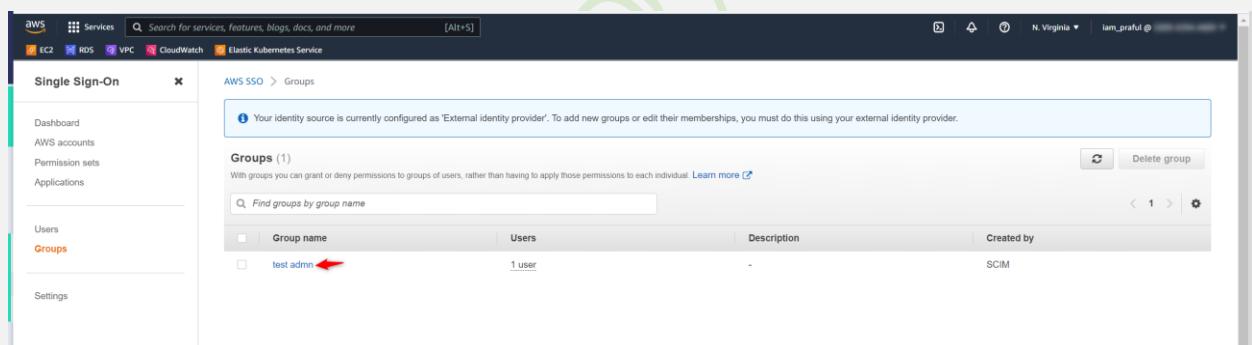
Verify sync status

AWS PROJECT
CYBERARK WORKFORCE IDENTITY

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH
IMPLEMENTED
BY: PRAFUL PATEL

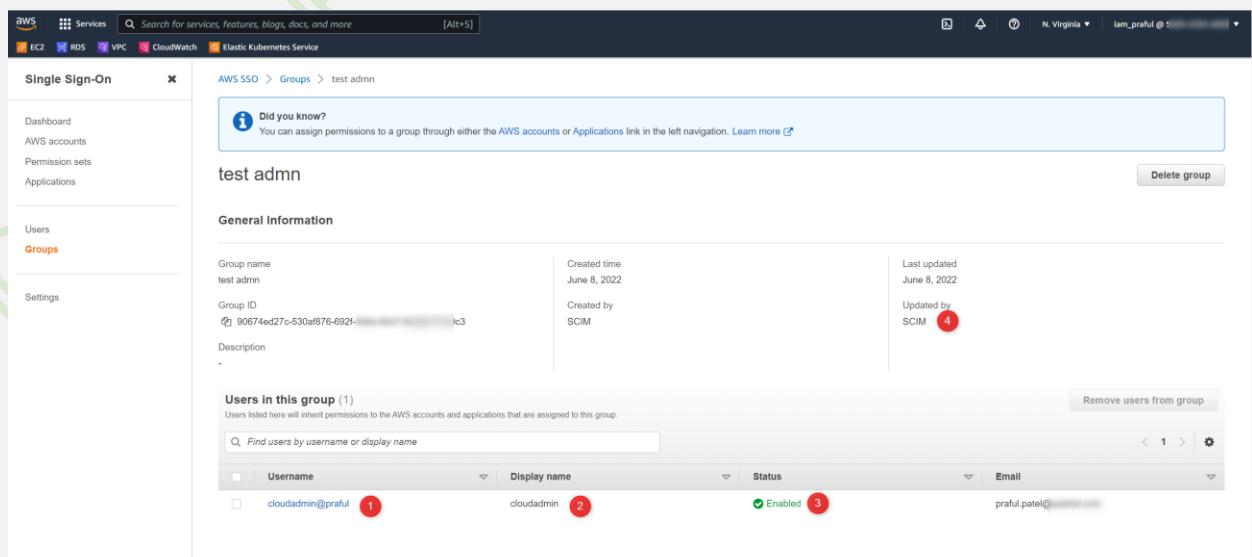
Type	Description	Submitted	Started	Completed	Status	Items Synced	Items Failed	Items Up To Date
Full Provisioning Sync	Full provisioning sync of other resources for AWS Single Sign-On (SSO)	06/08/2022 12:08 ...	06/08/2022 12:08 ...	06/08/2022 12:08 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of users for AWS Single Sign-On (SSO)	06/08/2022 12:08 ...	06/08/2022 12:08 ...	06/08/2022 12:08 ...	Completed	1	0	0
Full Provisioning Sync	Full sync of all provisioning enabled apps	06/08/2022 12:08 ...	06/08/2022 12:08 ...	06/08/2022 12:08 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of other resources for AWS Single Sign-On (SSO)	06/08/2022 12:08 ...	06/08/2022 12:08 ...	06/08/2022 12:08 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of users for AWS Single Sign-On (SSO)	06/08/2022 12:08 ...	06/08/2022 12:08 ...	06/08/2022 12:08 ...	Completed	0	0	1
Full Provisioning Sync	Full sync of all provisioning enabled apps	06/08/2022 12:08 ...	06/08/2022 12:08 ...	06/08/2022 12:08 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of other resources for AWS Single Sign-On (SSO)	06/08/2022 11:57 ...	06/08/2022 11:57 ...	06/08/2022 11:57 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of users for AWS Single Sign-On (SSO)	06/08/2022 11:57 ...	06/08/2022 11:57 ...	06/08/2022 11:57 ...	Completed	1	0	0
Full Provisioning Sync	Full sync of all provisioning enabled apps	06/08/2022 11:57 ...	06/08/2022 11:57 ...	06/08/2022 11:57 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of other resources for AWS Single Sign-On (SSO)	06/08/2022 11:53 ...	06/08/2022 11:53 ...	06/08/2022 11:53 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of users for AWS Single Sign-On (SSO)	06/08/2022 11:53 ...	06/08/2022 11:53 ...	06/08/2022 11:53 ...	Completed	0	0	0
Full Provisioning Sync	Full sync of all provisioning enabled apps	06/08/2022 11:53 ...	06/08/2022 11:53 ...	06/08/2022 11:53 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of other resources for AWS Single Sign-On (SSO)	06/08/2022 11:48 ...	06/08/2022 11:48 ...	06/08/2022 11:48 ...	Completed	0	0	0
Full Provisioning Sync	Full provisioning sync of users for AWS Single Sign-On (SSO)	06/08/2022 11:48 ...	06/08/2022 11:48 ...	06/08/2022 11:48 ...	Completed	0	0	0

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



The screenshot shows the AWS Single Sign-On Groups page. A red arrow points to the 'test admin' group name in the list.

Group name	Users	Description	Created by
test admin	1 user	-	SCIM



The screenshot shows the details for the 'test admin' group. A red circle with the number 4 is on the 'Last updated' row.

Group name	Created time	Last updated
test admin	June 8, 2022	June 8, 2022
Group ID	90674ed27c-530af876-692f-4c3	Created by SCIM
Description	Updated by SCIM	

Users in this group (1)

Username	Display name	Status	Email
cloudadmin@praful	cloudadmin	Enabled	praful.patel@...

AWS PROJECT
CYBERARK WORKFORCE IDENTITY

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH
IMPLEMENTED

BY: PRAFUL PATEL

The figure consists of three vertically stacked screenshots:

- Screenshot 1: AWS SSO Groups**
Shows the AWS SSO Groups page with two groups listed: "test admin" and "aws dev". Both groups have 1 user assigned.
- Screenshot 2: Gmail inbox**
Shows an incoming email from "CyberArk Account Management" with the subject "CyberArk Identity Service - User Account". The email body contains a CyberArk Identity welcome message, account details (login name: ays@praful), and a "Login Now" button.
- Screenshot 3: AWS SSO Users**
Shows the AWS SSO Users page with two users listed: "cloudadmin@praful" and "ays@praful". Both users are marked as "Enabled" and were created via SCIM.

Name ↑	Role Type	Description	Organization
aws dev	Static		
2 AWS test role	Static	This is just testing of AWS SSO with Cyberark	praful-org
CyberArk Remote Access Admin Users	Static	The read-only administrative role that allows access to the CyberArk Remote Access Admin Portal. Me...	
CyberArk Remote Access Users	Static	The default role that allows employee users to remotely access critical internal systems managed by C...	
Everybody	Static	All users are in this role by default, whether they have been added directly to the CyberArk Cloud Direc...	
SWS Admin	Static	Secure Web Sessions administrative role.	
SWS Auditor	Static	Secure Web Sessions auditor role.	
3 System Administrator	Static	The primary administrative role for the Admin Portal. Users in this role can delegate specific administr...	

Login Name ↑	Display Name	Email	Source	Organiz...	Status	Last Inv...	Last Login
1 ays@praful	ays	aysteller1@gmail...	CyberArk Cloud Directory	praful...	Invited	06/08/...	
2 cloudadmin...	cloudadmin	praful.patel@sas...	CyberArk Cloud Directory		Active	06/08/2022 9...	
3 tester@praful	tester	tester@gmail.com	CyberArk Cloud Directory		Invited	06/08/...	

All Interactive Users

- All Users
- Active Directory Users
- All Active Users
- All Invited Users
- All Non-Active Users
- All Service Users
- Azure Active Directory Users
- CyberArk Cloud Directory Users
- Federated Users
- Google Directory Users
- LDAP Users

Assign permission to user and group

Assigned users and groups (2)		
The following users and groups can access this AWS account from their user portal. Learn more		
<input type="text" value="Find users by username, find groups by group name"/>		
Username / group name	Permission sets	Type
cloudadmin@praful	AdministratorAccess	User
aws dev	AdministratorAccess	Group

AWS PROJECT CYBERARK WORKFORCE IDENTITY

FEDERATED ACCESS TO AWS SINGLE SIGN-ON WITH IMPLEMENTED BY: PRAFUL PATEL

The screenshot shows the AWS SSO console with the navigation path: AWS SSO > AWS accounts > praful_devops. The main view is the 'Overview' section for the 'praful_devops' account. Key details shown include:

- Account name: praful_devops
- Account ID: 500942944689
- Email: praful.biz2018@gmail.com

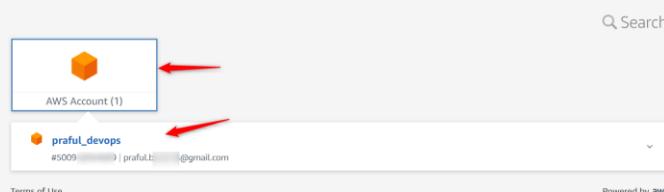
In the 'Permission sets' section, there is one permission set listed:

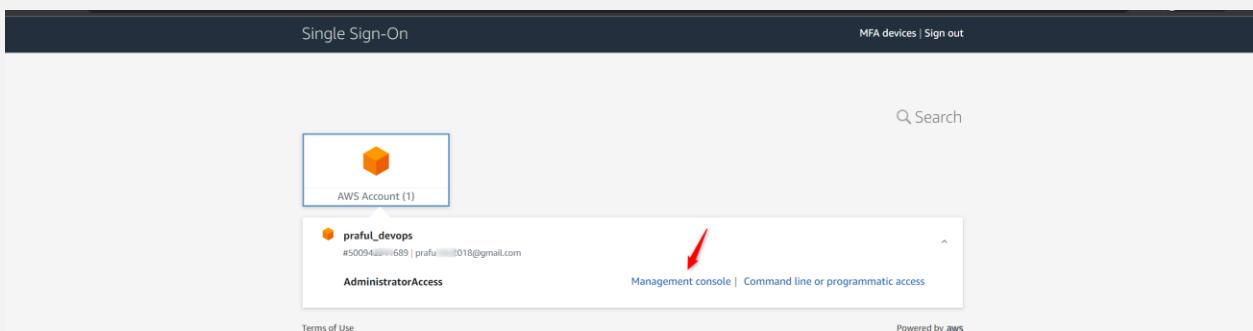
- Permission set: AdministratorAccess

Go to Cyberark user login

The screenshot shows the CyberArk Identity User Portal interface. The left sidebar has sections for Applications, Secured Items, Devices, Activity, and Account. The 'Applications' section is currently active. A red arrow points to the 'AWS Single Sign-On (SSO)' application icon. To its right is the 'Amazon Web Services (AWS)' application icon.

Below the portal interface, a browser window displays the AWS Single Sign-On login page. The URL is d-90674ed27c.awsapps.com/start#. The page shows the user is signed in to an AWS account, with a red arrow pointing to the 'AWS Account (1)' section. Another red arrow points to the user's email address, 'praful.t...@gmail.com', in the sign-in dropdown.





User is logged in using cyberark identity in AWS SSO

The screenshot shows the AWS Management Console home page. At the top, it displays the URL "us-west-2.console.aws.amazon.com/console/home?region=us-west-2#". The top navigation bar includes "AWS", "Services", "Search for services, features, blogs, docs, and more", and "[Alt+S]". On the far right, it shows "Oregon" and "AdministratorAccess/cloudadmin@praful.patel". A blue banner at the top states: "The new AWS Console Home will replace your existing experience soon. Starting June 2022, the new AWS Console Home will replace your current experience. Switch now to customize your Console Home and view valuable insights. Learn more or let us know what you think." A red arrow points to the "Switch now" button. The main content area is titled "AWS Management Console". It features sections for "AWS services", "Build a solution", and "Explore AWS". The "Build a solution" section contains eight items with icons and descriptions: "Launch a virtual machine" (With EC2, 2-3 minutes), "Build a web app" (With Elastic Beanstalk, 6 minutes), "Build using virtual servers" (With Lightsail, 1-2 minutes), "Register a domain" (With Route 53, 3 minutes); "Connect an IoT device" (With AWS IoT, 5 minutes), "Start migrating to AWS" (With AWS MGN, 1-2 minutes), "Start a development project" (With CodeStar, 5 minutes), and "Deploy a serverless microservice" (With Lambda, API Gateway, 2 minutes). The "Explore AWS" section includes links for "New AWS Console Home", "Stay connected to your AWS resources on-the-go", "Free AWS Training", "AWS Certification", and "Free Cloud Training Resources".

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



Congratulations!!!! 🎉