aws marketplace

Implementation Guide:

CyberArk Identity as Single Sign-on (SSO) for AWS Control Tower

CYBERARK®

Table of Contents

Foreword 3

Solution overview and features 4

Architecture diagram 4

Pre-requisites 5

Deployment and Configuration Steps 6

Solution Estimated Pricing 14

FAQs 14

Additional resources 14

Partner contact information 14

Foreword

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the CyberArk Identity's single sign-on (SSO) in AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

AWS Control Tower provides the easiest way to set up and govern a secure, multi-account AWS environment, called a landing zone. A landing zone is a well-architected, multi-account AWS environment that's based on security and compliance best practices. AWS Control Tower automates the setup of a new landing zone using best-practices blueprints for identity, federated access, and account structure. AWS Control Tower create a multi-account environment using AWS Organizations and provides identity management using AWS Single Sign-On (SSO) default directory.

AWS SSO is a cloud service provided by Amazon that allows you to grant user access to AWS resources, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, across multiple AWS accounts. AWS SSO centralizes the administration of users and permission sets across multiple AWS accounts. This enables administrators to establish federation with an Identity Provider (IdP) once and manage access to AWS.

CyberArk Identity integrates with AWS SSO as an identity provider for AWS Control Tower, automatically provisioning users, and groups to provide simplified secure user access to authorized AWS accounts and resources.

Architecture diagram

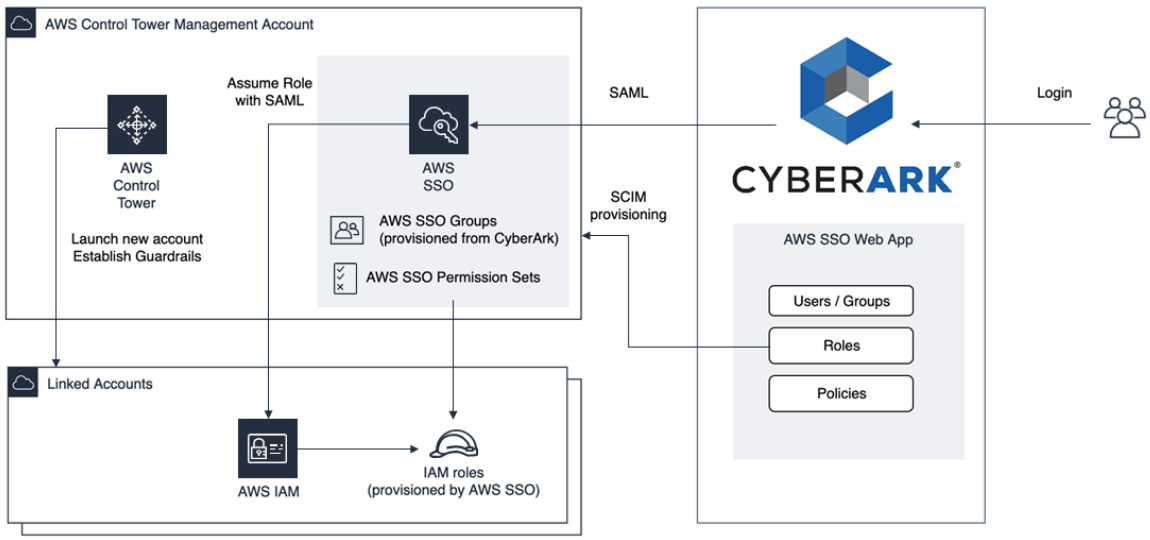


Figure 1 CyberArk Identity as SSO for AWS Control Tower - Architecture Diagram

AWS Control Tower automates new account provisioning in the organization with prescriptive and detective guardrails. AWS Control Tower also centralizes logging from AWS CloudTrail and AWS Config, and provides

protective and detective guardrails. The guardrails are AWS best practice settings and AWS Control Tower is designed to monitor and report the compliance status to a central console dashboard.

CyberArk acts as the external IdP for AWS Control Tower through integration with AWS SSO. This eliminates the need to manage user information in multiple places and allows you to centralize it with CyberArk. All users, groups and roles are managed within CyberArk and synchronized with AWS SSO directory by using System for Cross-domain Identity Management (SCIM). User attributes such as first name, last name, email and display name can be synchronized as well. Roles from CyberArk are synchronized as group in AWS SSO directory. Administrator can select combination of users or groups and AWS SSO Permission sets, then assign it to the relevant AWS accounts.

Users authenticates to CyberArk portal and the relevant CyberArk policies are applied. For example, rule filter based on IP address, day or time range, device OS, browser, devices, MFA, etc. From CyberArk portal, user navigate to AWS SSO by using the assigned web apps. CyberArk sent the SAML assertion to authenticate the user with AWS SSO. Once in AWS SSO, user select the target AWS account and login using the available permission sets.

Pre-requisites

Before you configure the CyberArk Identity integration with AWS Control Tower and AWS SSO, you need to deploy AWS Control Tower or have AWS SSO enabled in your AWS Organization management account. To get started with AWS Control Tower, check out the getting started with Control Tower

This guide assume you already have CyberArk Identity account / subscription. You can acquire CyberArk Identity account from the following:

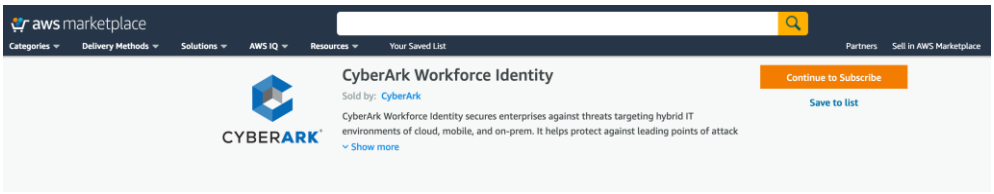
- CyberArk Workforce Identity on AWS Marketplace
- CyberArk Identity free trial sign-up

Instructions for AWS Marketplace are available in the following section. Click here for additional information on AWS Marketplace. if you are new to AWS, see Getting Started with AWS.

Deployment and Configuration Steps

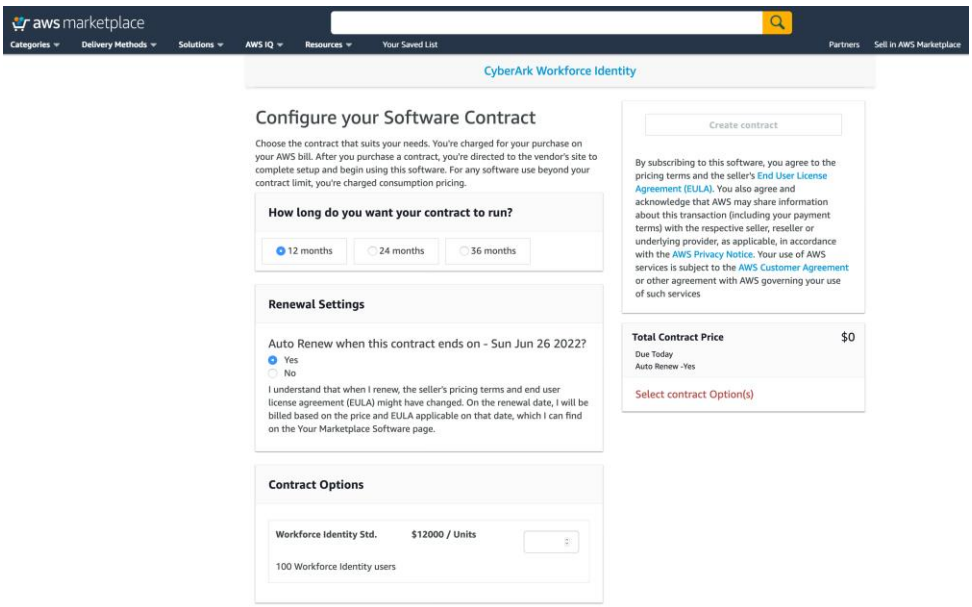
Step 1: Optional: Subscribe to CyberArk on AWS Marketplace

If you already have CyberArk account, please continue to step 2. To subscribe for CyberArk, browse for [CyberArk Workforce identity on AWS Marketplace]



Choose the **Continue to Subscribe** button.

In the new screen, you can configure your contract. You can select the **Contract Duration**, **Renewal Settings** and **Contract Options**.

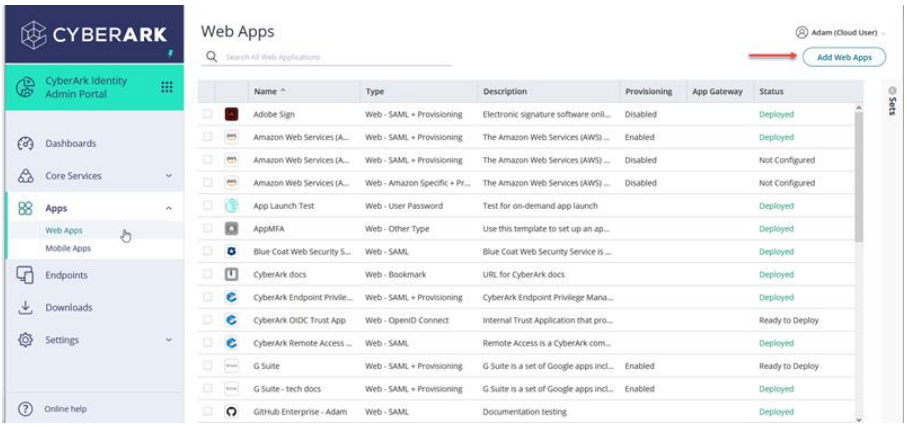


Once you have configured your contract, you can select the **Create contract** button. Once you agree to **Pay Now**, follow the instruction to complete the sign up.

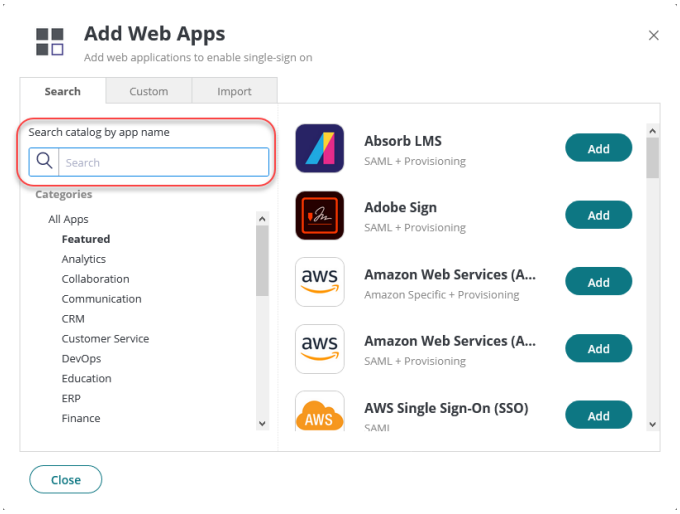
Step 2: Add the AWS Single Sign-On application in the Admin Portal.

1. Login to CyberArk admin portal.
2. In the Admin Portal, select **Apps > Web Apps**, then click **Add Web Apps**.

   The Add Web Apps screen appears.



3. On the Search tab, enter **AWS Single Sign-On (SSO)** in the **Search** field and click the search icon.



3. Next to the application, click **Add**.
4. In the Add Web App screen, click **Yes** to confirm.
5. Click **Close** to exit the Application Catalog.

   The application that you just added opens to the Settings page.

Step 3: Access the AWS Management Console Single Sign-On page to enable an external identity provider.

1. Open a new tab in your web browser, then go to the AWS Management Console and sign-in to your AWS Control Tower management account.
2. Under Security, Identity, & Compliance, click **AWS Single Sign-On**.

3. Click **Settings**, and then click **Change** next to Identity Source.

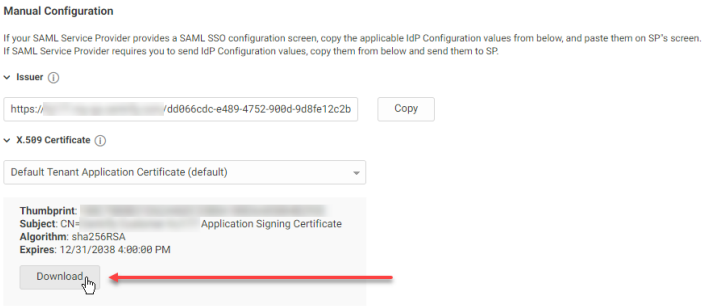
4. Under Choose where your identities are sourced, click **External identity provider**.

Step 4: Select the Trust page in the Admin Portal to configure IdP and Service Provider information.

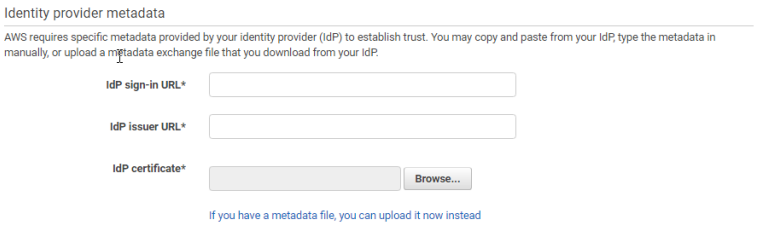
1. Return to CyberArk Admin Portal.

2. Click the Trust page in the Admin Portal, and then select **Manual Configuration** in the IdP Configuration area to access the configuration content required in the AWS Management Console.

2. In the IdP Configuration area of the Trust page, expand the certificate area and select the certificate that you want to use for the application, then click **Download**.



3. In the AWS Management Console, navigate to the Identity provider metadata section, and then select the link, **if you don't have a metadata file, you can manually type your metadata values**. The following screen appears.



4. Next to IdP certificate*, click **Browse** and then select the file you downloaded from the Admin Portal.

5. Configure the following additional IdP fields:

Admin Portal Option	Configuration
Single Sign on URL	Copy the URL from the Admin Portal Trust page into the IdP sign-in URL field in the AWS Management Console. (The CyberArk Identity generates the content for this field.) Note: When a user goes to the AWS URL, AWS has the CyberArk Identity authenticate the user. If the user isn't already logged in to the User Portal, then the CyberArk Identity prompts the user to log in. If the user is already logged in to the User Portal, then the CyberArk Identity authenticates the user and logs the user in to AWS.
IdP Entity ID / IdP Issuer	Copy the URL from the Admin Portal Trust page into the corresponding field in the into the IdP sign-in URL field in the AWS Management Console. (The CyberArk Identity automatically generates the content for this field.)

6. In the AWS Management Console, navigate to the Service provider metadata section, and click **Download metadata file**.

7. In the Admin Portal **Service Provider Configuration** area, select **Metadata > Choose File** and then select the file you downloaded from the AWS Management Console.

8. In the Admin Portal, click **Save**.

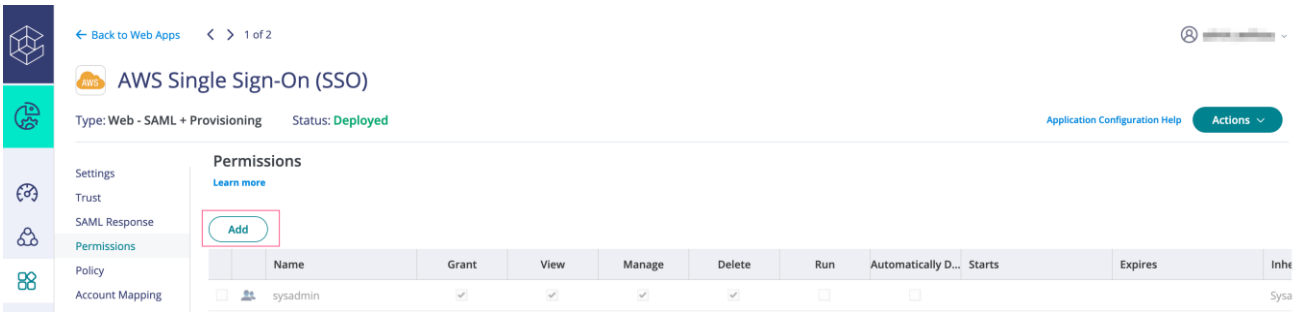
9. In the AWS Management Console, click **Next: Review** and review your changes, enter **CONFIRM** and then click **Finish**.

   Note: *SP-initiated SSO:* Users can access the AWS Single Sign-On application directly and authenticate with the CyberArk Identity using the User portal URL link in the AWS Management Console > Security, Identity, & Compliance > AWS Single Sign-On > Settings page.

Step 5: Set permissions or add the application to a set to deploy the application to users.

1. Return to CyberArk Admin portal

2. On the Permissions page, click **Add**.



2. Select the user(s), group(s), or role(s) that you want to give permissions to, then click **Add**.
   The added object appears on the Permissions page with View, Run, and Automatically Deploy permissions selected by default.

3. Select the desired permissions, then click **Save**.
   Default permissions will automatically deploy the application to the User Portal. Change the permissions if you want to add additional control or you prefer not to automatically deploy the application.

   Refer to the following table for more information about applications-specific permissions.

Permission	Description
Manage	Users can modify application settings and application sets. Selecting this option also selects the View permission. Additionally, a user in a role with the Application Management administrative right can enable this permission to allow other users or roles (without the Application Management right) to administer the application. See Delegate application management for more information. Note that you cannot delete applications from the Admin Portal > Web Apps and Mobile Apps pages with just this permission. Add the **Delete** permission if you want a delegated application administrator to have the ability to delete applications.

Permission	Description
Delete	Users with this permission can delete applications from the Admin Portal > Web Apps and Mobile Apps pages. Selecting this option also selects the View permission.
Run	Allows users to launch the application from the User Portal.
Automatically Deploy	Automatically deploys the application to the User Portal. If Automatically Deploy is not selected, users can find the application in the Recommended tab when adding applications to the User Portal.

Step 6: Enable SCIM provisioning in AWS SSO

SCIM is an open standard for automating the exchange of user identity information between identity domains, or IT systems. It can be used to automatically provision and deprovision accounts for users in external systems such as your custom SAML app. For more information about SCIM, see www.simplecloud.info.

1. Return to AWS Management Console and select AWS SSO, navigate to the **Settings** page.
2. Under **Provisioning** select **Enable automatic provisioning**.
3. Select S**how token** to expand the access token.
4. Copy both the SCIM endpoint URL and Access token, you will need it on the next section.

Step 7: Enable SCIM provisioning in CyberArk

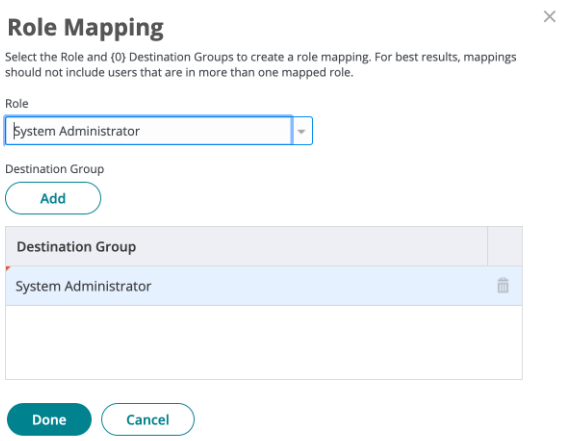
1. In the CyberArk Admin Portal, select **AWS Single Sign-On (SSO)** app and go to the **Provisioning** page.
2. Select **Enable provisioning for this application.**
3. Under **SCIM Service URL** enter the SCRIM endpoint URL from the previous section.
4. Under **Authorization Type**, select **Authorization Header**

5. Under **Bearer Token**, enter the Access token from the previous section.

6. Choose **Verity** to test connectivity.
7. Under **Sync Options** select the appropriate config as per your requirements.
8. Navigate to the Role Mappings section.
9. Click **Add** to open the Role Mapping dialog box.
10. Select a **Role**.
11. Click **Add** and select a **Destination Group** from the drop-down list.

    If the Destination Group is selected, a group with that name is created in the AWS SSO. If you select a Destination Group that already exists in the AWS SSO, provisioned users that are members of the selected role are added as members of the existing Destination Group. Alternatively, you can type in a new group name to map to the selected role

    If the role is removed from the role mapping after a provisioning job runs, the Destination Group remains in the AWS SSO without any membership changes. Changing the role or role name does not affect Destination Group creation or membership, unless the Destination Group name in the role mapping is also changed.
12. (Optional) Add more Destination Groups, if desired, by repeating the previous two steps.



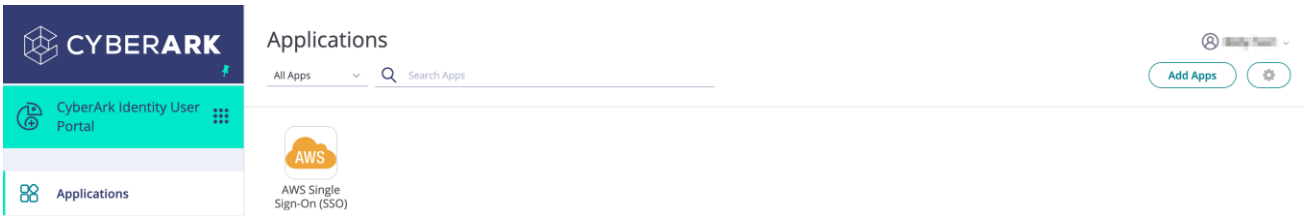
13. Click **Done** to save the role mapping and return to the Provisioning page.
14. Continue adding role mappings, as desired.

Step 8: Assign AWS SSO Permission Sets

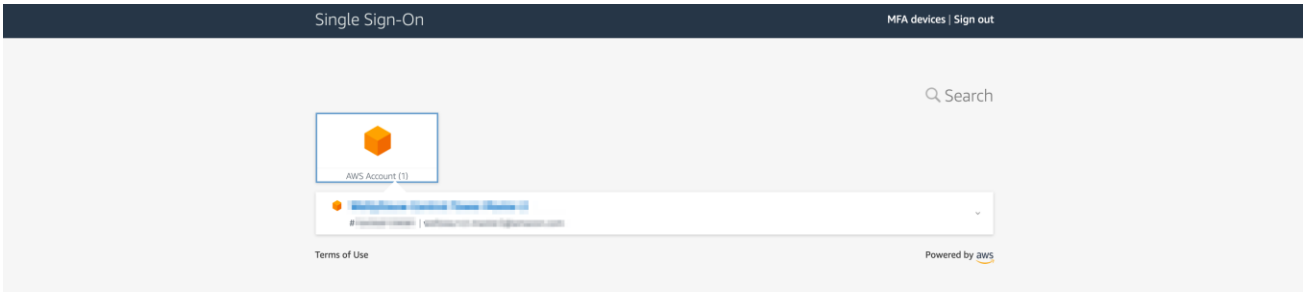
1. In the AWS Management Console, navigate to **AWS SSO.**
2. Select **AWS Accounts** page from the left navigation pane, select the **AWS organization**
3. Select the AWS account you want to assign to the group choose **Assign users**.
4. In the **Assign Users page**, select the group from the CyberArk role mapping earlier. If the group is not found:
    - Refresh the AWS SSO page.
    - Re-run synchronization by following the CyberArk guideline provisioned account synchronization options.
5. Choose **Next: Permission sets**.
6. Under the **Select Permission Sets** section, select the permission set you want to assign to the group. If you don't have an existing permission set, choose **Create New Permission Set.**
7. Click **Finish.**

Step 9: Test CyberArk integration with AWS Control Tower and AWS SSO

Login to CyberArk user portal using user member of the role that you assigned previously. Select the **AWS Single Sign-On (SSO)** from the application list.



Upon successful authentication, you will be prompted to AWS SSO landing page.



Solution Estimated Pricing

There is no additional charge to use AWS Control Tower. However, when you set up AWS Control Tower, you will begin to incur costs for AWS services configured to set up your landing zone and mandatory guardrails. Please refer to example pricing for AWS Control Tower for more detail.

There is no additional cost for using the AWS SSO for integration with CyberArk.

For detail cost of CyberArk solution, please refer to the AWS marketplace pricing information for CyberArk Workforce Identity

FAQs

Refer to CyberArk customer support page for further detail about the product.

Additional resources

- Integrate AWS Single Sign-On (SSO) into CyberArk
- Configuring AWS CLI to use AWS SSO
- Attribute based access control (ABAC) with AWS SSO

Partner contact information

For further information about this solution and CyberArk, contact: bizdevtech@cyberark.com