



SECURING ACCESS TO THE AWS CONSOLE WITH ZERO STANDING PRIVILEGE USING CYBERARK SECURE CLOUD ACCESS (SCA)

PREREQUISITES:

Client Workstation Requirements

Modern Browser like Chrome/Edge/Firefox
Internet access

CyberArk Lab

Your CyberArk instructor will provide the CyberArk lab link via chat


SECTION 1: LOG IN AND CREATE AN SCA POLICY FOR GRANTING ACCESS

Sign into the CyberArk Identity Security Platform

In this section, you will be guided through logging into the CyberArk Identity Security Platform which includes the Secure Cloud Access capabilities being discussed today. The Identity Security Platform enables operational efficiencies, leveraging a single admin portal with unified audit and Identity Security Intelligence.


1. Login to the Identity Portal link provided by your instructor

A screenshot of the CyberArk Identity Security Platform login interface. It features the CyberArk logo at the top left, followed by the text "Sign In". Below this is a prompt "Enter your username (user@domain)" and a text input field containing "test.user@sca.cloud". A blue "Next" button is positioned below the input field.

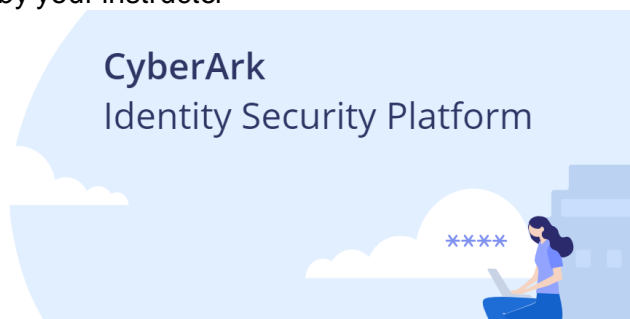
 **CYBERARK**

Sign In

Enter your username (user@domain)

 test.user@sca.cloud

Next

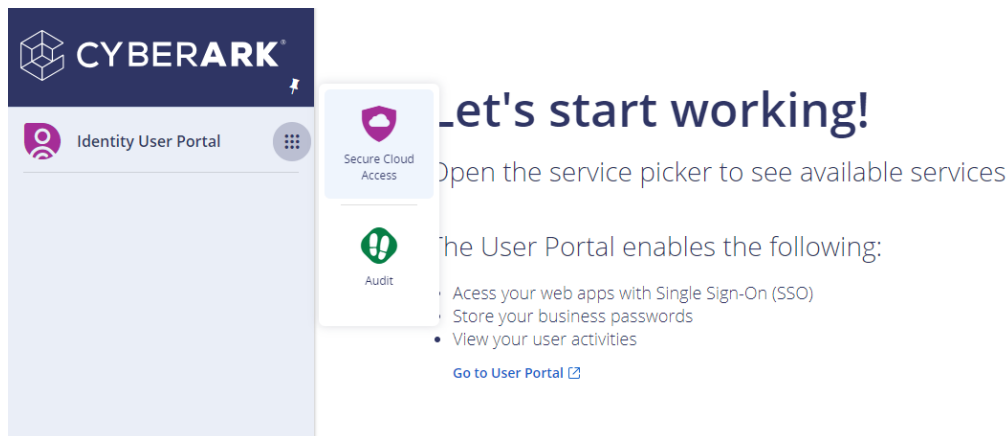


2. Your username is the first part of the email you used to register with followed by @sca.cloud
 - a. For example, if you registered with johnsmith@company.com , use johnsmith@sca.cloud
3. Password will be shared by the instructor during the lab session

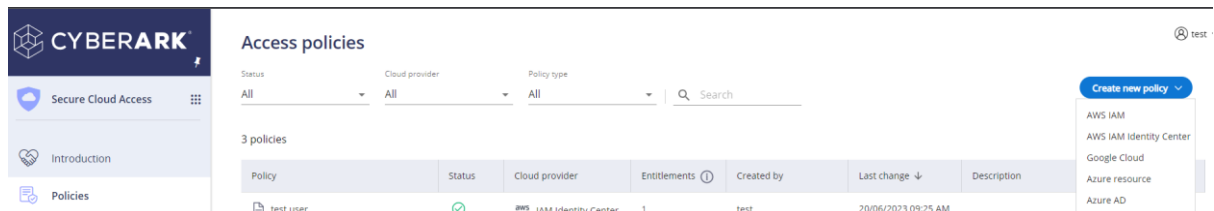
Create a Secure Cloud Access policy

In this section, you will be acting as a cloud security architect defining access to the AWS console. You will create a Secure Cloud Access policy which will grant a user (developer, devops engineer, SRE, etc.) the ability to elevate access to the AWS console just in time. The assigned user continues to have zero standing privilege until they actively use the policy you create in this step.

1. Choose the service selector in the top left corner, and select Secure Cloud Access



2. Select Policies on the left-hand side
3. Select Create new policy on the top right and choose AWS IAM Identity Center



- a. General Details:
 - i. Policy name: Your "FirstnameLastname Policy"
 - ii. Description: Optional
 - iii. Policy Time Frame: Never Expires
- b. Cloud Permission Sets:
 - i. Click accounts and permission sets
 - ii. Select any account on the left-hand side (This is the account or accounts you will be granting access)
 - iii. Check the box for a permission set but **please do not select** CyberArkAdministratorAccess (It will not work)
 - iv. Click Select
- c. Access Rules:
 - i. Click Add Identities
 - ii. In "search for an identity" type in the username you logged in with
 - iii. Check the box for your user
 - iv. Click Add to policy
 - v. Make note that you can change the maximum session length

- vi. Uncheck Saturday and Sunday to create a policy that is only accessible Monday thru Friday
- vii. Select “all day” as the time frame
- d. Save the policy

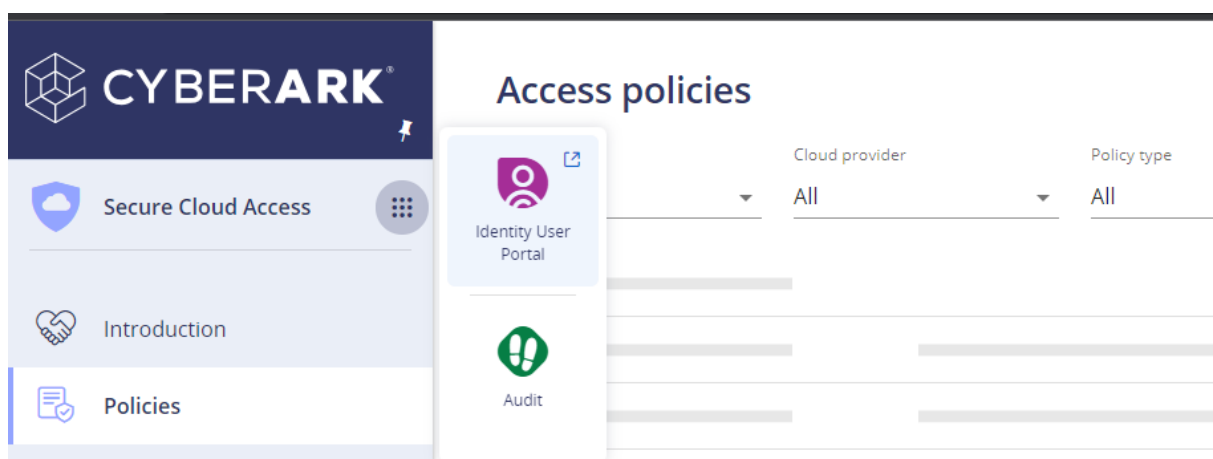
You have now created a policy that will elevate a user or group of users’ permission from zero standing privilege to exactly what they need just in time! Permissions will automatically deprovisioned when the defined session length expires.

SECTION 2: ACCESS THE AWS CONSOLE USING THE SECURE CLOUD ACCESS POLICY

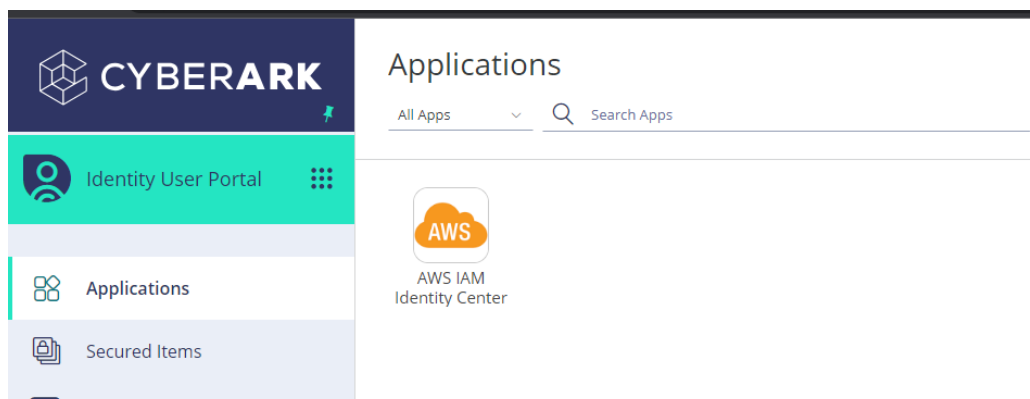
Log into the AWS Console

In this section, you will act as a user who needs privileged access to the AWS Console or CLI (think someone like a developer, devops engineer, or SRE). The user will elevate their access JIT using the policy you created in the previous step.

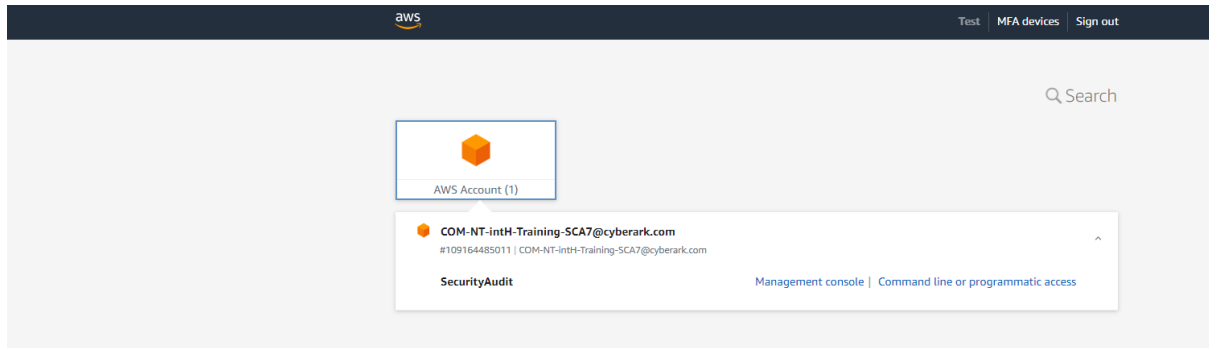
1. In your web browser, click on the service selector icon and choose Identity User Portal



2. Select the AWS IAM Identity Center web application



3. Hover over the permission set that you granted access to via the policy you created in section 1 and click connect
4. In the AWS SSO Page, click “AWS Account”
 - a. Click the AWS account that appears
 - b. Click management console next to the permission set you requested access to (notice that you could also connect via command line (CLI))



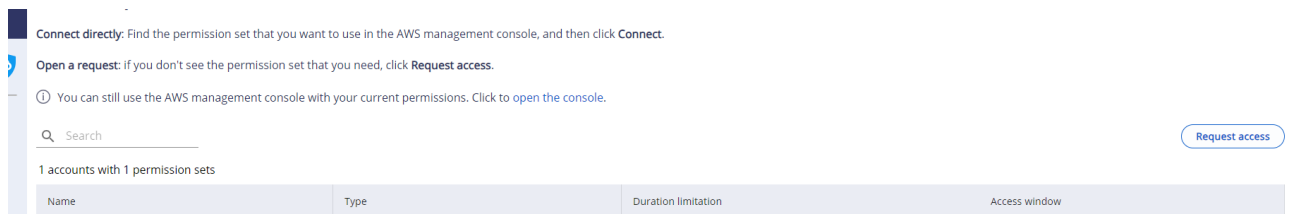
You are now logged into that account with the permission set assigned as requested. Your access to this permission set will automatically be deprovisioned when the session duration limit is reached!

SECTION 3: REQUEST ACCESS ON DEMAND

Create an On Demand Request

In this section, the user will request on demand access to an AWS account/permission set that has not yet been defined via an access policy. This is an example of how a workflow request can be utilized to grant emergency access JIT.

1. Close the AWS Console
2. Navigate back to the Identity User Portal
3. Click the AWS IAM Identity Center web app
4. In the top right-hand corner, select Request Access



5. Fill in the request form accordingly:
 - a. Reason: Fill in any reason as needed
 - b. Ticket Number: Optional but can use this to audit against an open ticket
 - c. Account: Specify the account you need access to

- i. Use a different account than what you created in your access policy previously
 - ii. Instructor will provide a list of accounts on the screen that you can use
 - d. Permission Set: Specify the Permission Set you are requesting access to
 - i. Instructor will provide a list of permission sets you can request
 - e. Time Zone: Select your time zone
 - f. Date: Today's date
 - g. Select the current time and choose 1 hour for session length
 - h. Click Send Request
- 6. Your request has been sent using our workflow request process. The CyberArk team will approve these requests for the purpose of this lab.

Log into the AWS console using your on-demand access

Now that the access request has been granted, the user will proceed to connect.

1. Navigate back to the Identity User Portal
2. Click the AWS IAM Identity Center web app
3. Notice the new account/permission set is now available
 - a. Click connect on the right for this permission set
4. In the AWS SSO Page, click "AWS Account"
 - a. Click the AWS account that appears
 - b. Click management console next to the permission set you requested access to (notice that you could also connect via command line (CLI))