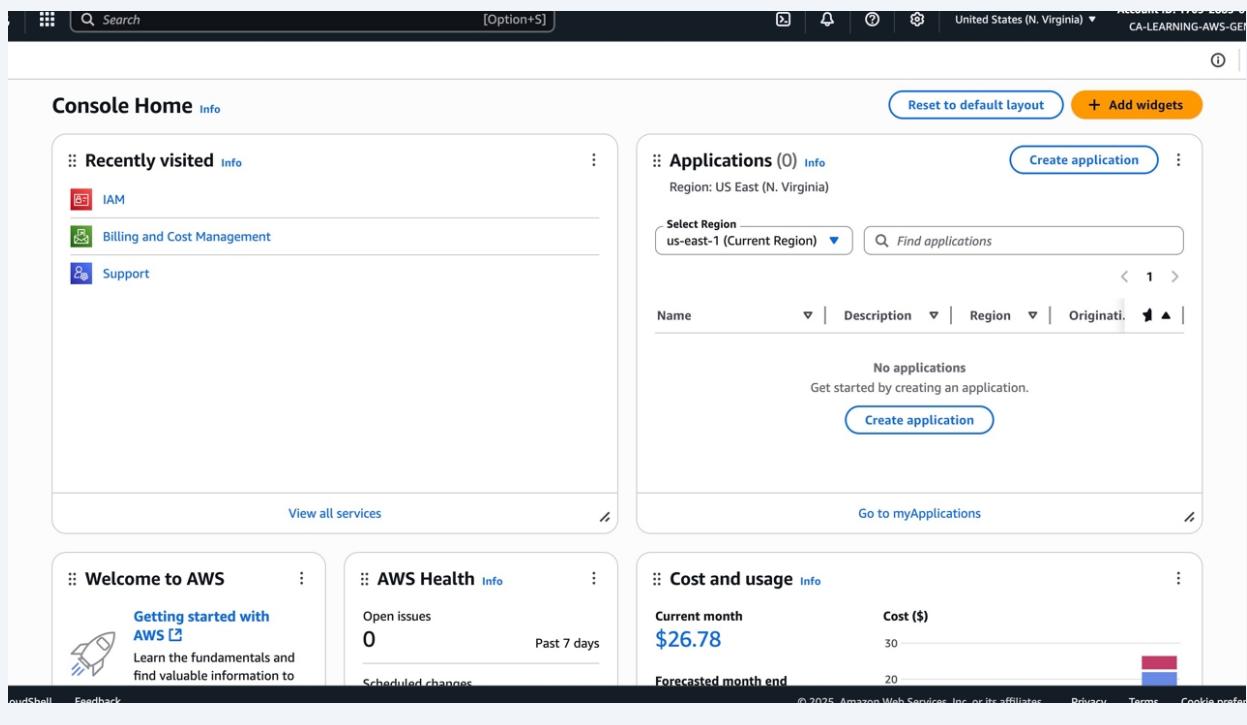


Adding and securing an IAM Admin user for the account.

1

Navigate to
<https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1>



The screenshot shows the AWS Console Home page. At the top, there is a navigation bar with a search bar, a [Option+S] button, and account information (Account ID: 1111222233445566, Region: United States (N. Virginia), and Account Name: CA-LEARNING-AWS-GEN). Below the navigation bar, the "Console Home" section is visible. On the left, a sidebar titled "Recently visited" lists services: IAM (selected), Billing and Cost Management, and Support. In the center, there are three main cards: "Applications (0)" which shows no applications and has a "Create application" button; "Welcome to AWS" which includes a "Getting started with AWS" link and a "Cost and usage" card showing current month costs at \$26.78 and forecasted month end costs at 20; and "AWS Health" which shows 0 open issues over the past 7 days. At the bottom, there are links for "View all services", "Go to myApplications", and footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

2 Click the "Search" field and type in "IAM".

The screenshot shows the AWS Console Home page. At the top, there is a search bar with the placeholder text "Search" and a magnifying glass icon. A yellow circle highlights this search bar. To the right of the search bar are account details: "Account ID: 1709" and "United States (N. Virginia)". Below the search bar, there are sections for "Recently visited" services (IAM, Billing and Cost Management, Support), "Applications" (0), "Welcome to AWS" (Getting started with AWS), "AWS Health" (Open issues 0), and "Cost and usage" (Current month \$26.78). A "View all services" button is located at the bottom left of the main content area.

3 Click on the "IAM" service

The screenshot shows the AWS search results page for the query "iam". The search bar at the top contains the text "iam". In the main content area, the "Services" section is expanded, showing the "IAM" service card. This card has a red circle highlighting its icon. The card title is "IAM Manage access to AWS resources" and it includes links for "Groups", "Users", "Roles", "Policies", and "Access Analyzer". Below this, there are sections for "Features" (IAM Access analyzer for S3, Groups, Roles) and a feedback section ("Were these results helpful?"). To the right of the search results, the same "Applications" and "Cost and usage" sections from the previous screenshot are visible.

4 Once you are on the IAM dashboard, click "Users"

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Tools'. The 'Users' link under 'Access management' is highlighted with an orange circle. The main content area has a blue header bar with the message 'New access analyzers available' and a 'Create new analyzer' button. Below this is the 'IAM Dashboard' section with 'Security recommendations' (2 items), 'IAM resources' (User groups: 0, Users: 0, Roles: 2, Policies: 0, Identity providers: 0), 'What's new' (View all), and 'AWS Account' details (Account ID: 170928836744, Account Alias: canks-learning-aws-general). There are also 'Quick Links' and 'Tools' sections.

5 Click on "Create user"

The screenshot shows the 'Users' page within the IAM service. The sidebar on the left includes 'Access management' and 'Reports'. The main area displays 'Users (0)' with a note: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A search bar is at the top. Below it is a table header with columns: 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in'. A large orange button labeled 'Create user' is prominently displayed on the right side of the page.

- 6 Click the "User name" field and type in "iamadmin".

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. The 'User name' field is highlighted with an orange circle. The field contains the text 'User name'. Below the field, a note says: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ _ - (hyphen)'. There is also an optional checkbox for providing console access.

- 7 Click the checkbox to provide the iamadmin user access to the AWS Management Console .

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. The 'User name' field contains the text 'iamadmin'. The 'Provide user access to the AWS Management Console' checkbox is highlighted with an orange circle. The checkbox is unchecked. Below the checkbox, a note says: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.'

8

Choose the radio button option "I want to create an IAM user". Later on we will use the other "User type".

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. In the 'User type' section, the radio button for 'I want to create an IAM user' is selected and highlighted with an orange circle. A tooltip explains that this is recommended for programmatic access through access keys or service-specific credentials.

9

For password, I chose the option to create a custom password.

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. In the 'Console password' section, the radio button for 'Custom password' is selected and highlighted with an orange circle. A tooltip indicates that a custom password must be at least 8 characters long and include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ - (hyphen) = [].

10

Type in your preferred password and uncheck the option to create a new password upon sign in.

Screenshot of the AWS IAM 'Create user' step 4 page. The 'Custom password' field is highlighted with a red circle. The page shows fields for user name, access type (selected 'I want to create an IAM user'), console password (selected 'Custom password'), and password creation options (unchecked 'Users must create a new password at next sign-in'). A note at the bottom suggests generating programmatic access.

11

Click "Next" to move on.

Screenshot of the 'Are you providing console access to a person?' step of the IAM user creation wizard. The 'Next' button is highlighted with a red circle. The page displays the same configuration as the previous screenshot, including user type, console password, and password creation options.

12

We will be attaching the permission policy directly so click this radio button with the option to do so..

The screenshot shows the 'Set permissions' step of the 'Create user' wizard. On the left, there are navigation links: 'user details', 'Permissions', 'and create', and 'password'. The main area is titled 'Set permissions' with the sub-instruction: 'Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions.' Below this is a 'Permissions options' section containing three radio buttons:

- Add user to group: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.'
- Copy permissions: 'Copy all group memberships, attached managed policies, and inline policies from an existing user.'
- Attach policies directly: 'Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.'

Below the options is a 'Get started with groups' section with a 'Create group' button. A note says: 'Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.' At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

13

Choose the "AdministratorAccess" permission policy..

The screenshot shows the 'Permissions policies' section with 1386 policies listed. The 'AdministratorAccess' policy is highlighted with a red circle. The list includes other policies like 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBean...', 'AIOpsAssistantPolicy', etc. At the top right are 'Create policy' and 'Attached entities' buttons. The bottom of the page includes links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and 'Privacy Terms Cookies'.

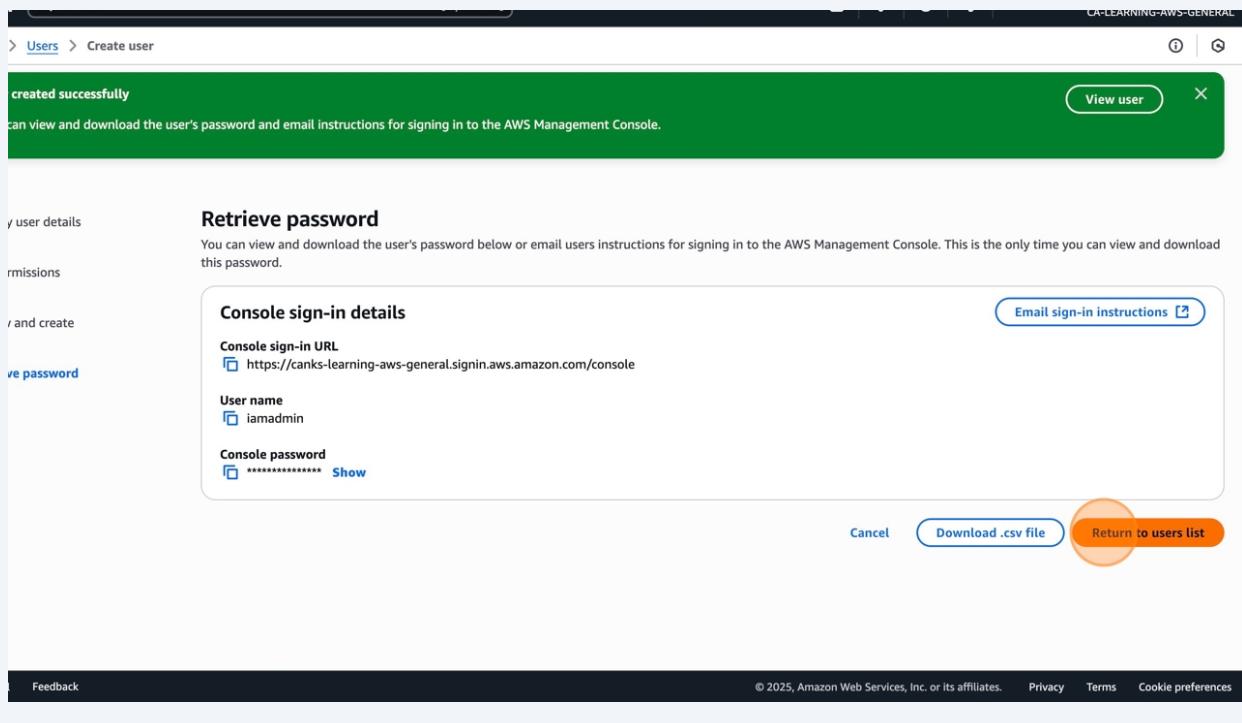
14 Click "Next"

The screenshot shows the 'Set permissions boundary - optional' step of the 'Create user' wizard. It lists various AWS managed permissions with checkboxes. A note below says: '▶ Set permissions boundary - optional'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being highlighted.

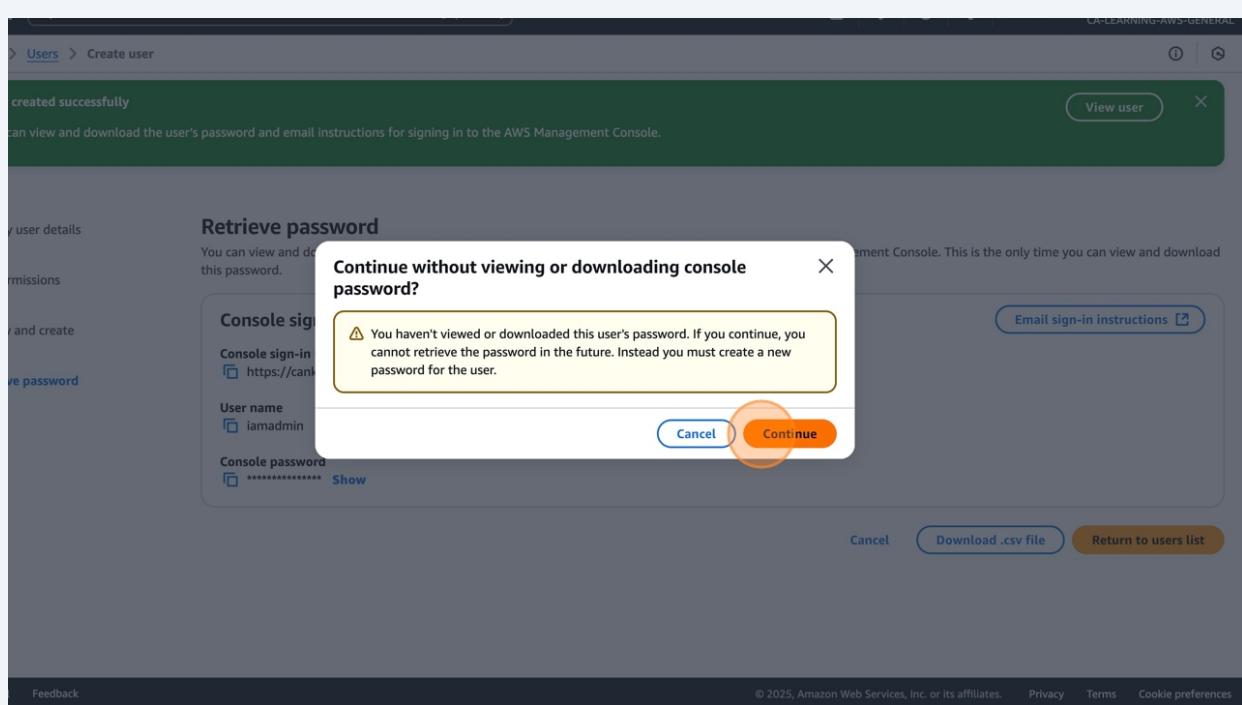
15 Click "Create user" to create the user.

The screenshot shows the 'Review and create' step of the 'Create user' wizard. It displays the user details (User name: iamadmin), a permissions summary (AdministratorAccess), and a tags section (No tags associated). At the bottom right are 'Cancel', 'Previous', and 'Create user' buttons, with 'Create user' being highlighted.

16 Click "Return to users list"



17 Click "Continue" to return to the Dashboard.



18 Click "Dashboard"

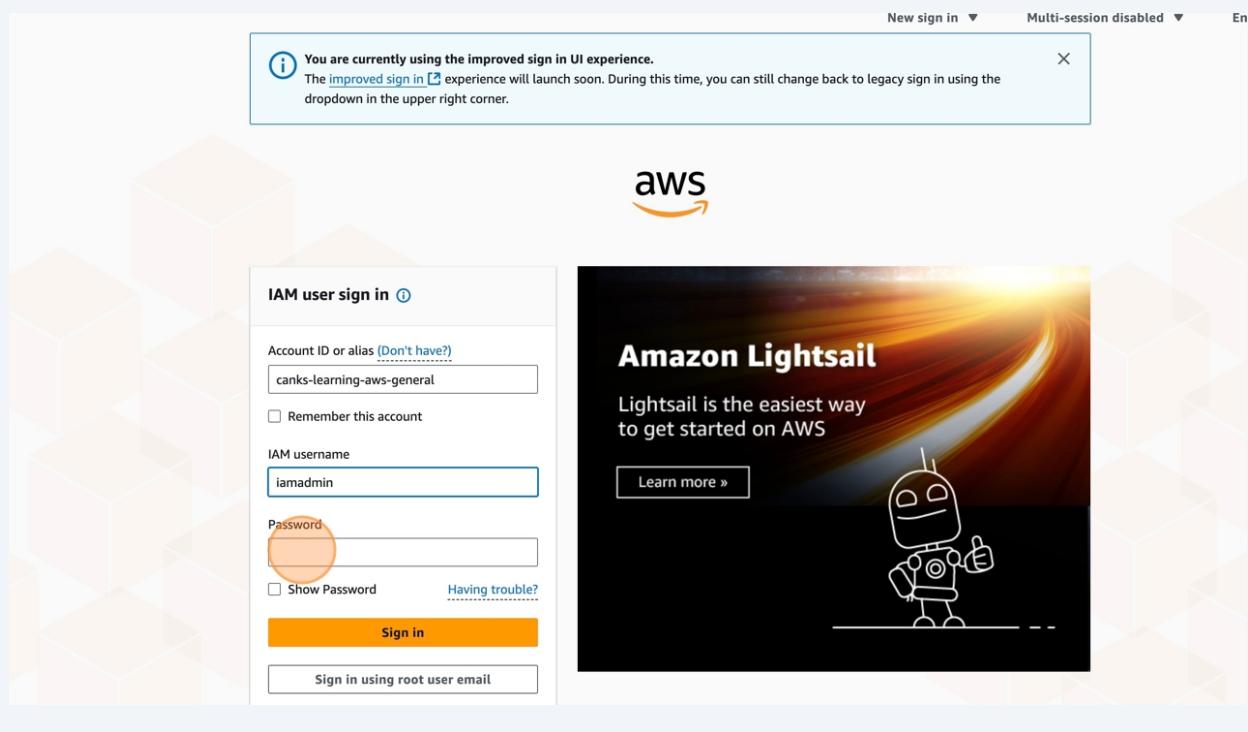
The screenshot shows the AWS IAM Users page. A green success message at the top states: "User created successfully. You can view and download the user's password and email instructions for signing in to the AWS Management Console." Below this, a table lists one user: "iamadmin". The table includes columns for User name, Path, Groups, Last activity, MFA, Password age, and Console last used. The "iamadmin" row has a single entry in the User name column. On the left sidebar, under "Access management", there is a link to "Sign-in URL for IAM users".

19 Copy the "Sign-in URL for IAM users" and paste in a new tab. NB: You will be signed out of your current tab.

The screenshot shows the AWS IAM Dashboard. In the top right corner, there is a box labeled "AWS Account" with the "Account ID" field containing "170928836744". Below it, the "Sign-in URL for IAM users in this account" is listed as "https://canks-learning-aws-general.signin.aws.amazon.com/console". This URL is circled in orange. The dashboard also features sections for "Security recommendations", "IAM resources" (with 1 user, 2 roles, and 0 policies), "What's new" (with updates about Amazon Bedrock and AWS Service Reference Information), and "Quick Links" and "Tools".

20

Fill in the the "IAM username" and "Password" fields and click "sign in".



21

The next step is to secure the "iamadmin" account just like we did for the "root user" account. Click on the account dropdown.

The screenshot shows the AWS Console Home page. At the top, there is a search bar, a "[Option+S]" keyboard shortcut, and a user dropdown for "canks-learning-aws-general (1709-2885-6744) iamadmin". Below the header, there are several cards: "Recently visited" (IAM), "Applications (0)" (Create application), "Welcome to AWS" (Getting started with AWS, Learn the fundamentals and find valuable information to), "AWS Health" (Open issues 0, Past 7 days, Scheduled changes), and "Cost and usage" (Current month \$26.78, Cost (\$), Forecasted month end 20). At the bottom, there are links for "View all services" and "Go to myApplications".

22 Click "Security credentials"

Console Home [Info](#)

Reset to default language

Account ID
1709-2883-6744

IAM user
iamadmin

Recently visited [Info](#)

IAM

View all services

Applications (0) [Info](#)

Region: Europe (Stockholm)

Select Region
eu-north-1 (Current Region) ▾

Find applications

Name | Description | Region

No applications

Get started by creating an application

Create application

Turn on multi-session support

Switch role Sign out

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to

AWS Health [Info](#)

Open issues 0 Past 7 days

Scheduled changes

Cost and usage [Info](#)

Current month \$26.78 Cost (\$)

Forecasted month end 20

23 Click "Assign MFA device"

> Security credentials

and Access management (IAM)

Console sign-in

Console sign-in link
<https://canks-learning-aws-general.signin.aws.amazon.com/console>

Console password
Updated 3 minutes ago (2025-08-23 01:20 GMT+1)

Last console sign-in
Now (2025-08-23 01:23 GMT+1)

[Update console password](#)

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
Assign MFA device			

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

[Create access key](#)

X.509 Signing certificates (0)

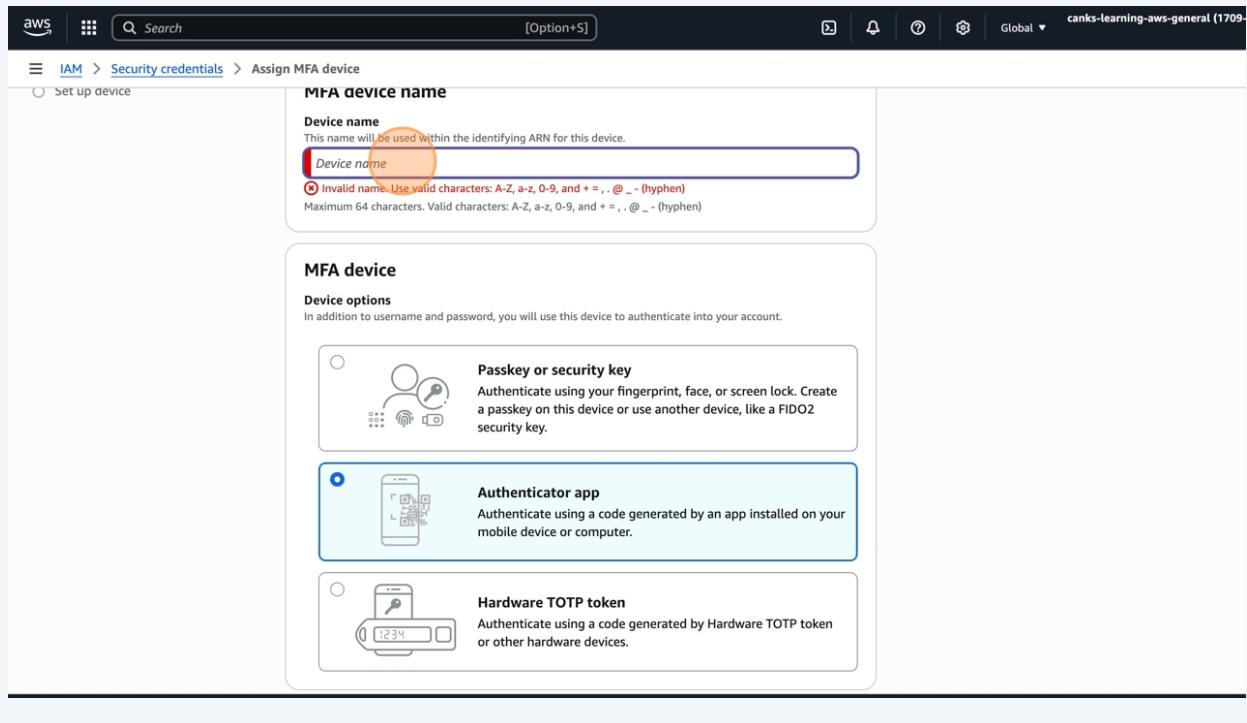
[Actions](#) [Upload](#) [Create X.509 certificate](#)

© 2025, Amazon Web Services, Inc. or its affiliates.

Feedback Privacy Terms Cookie preferences

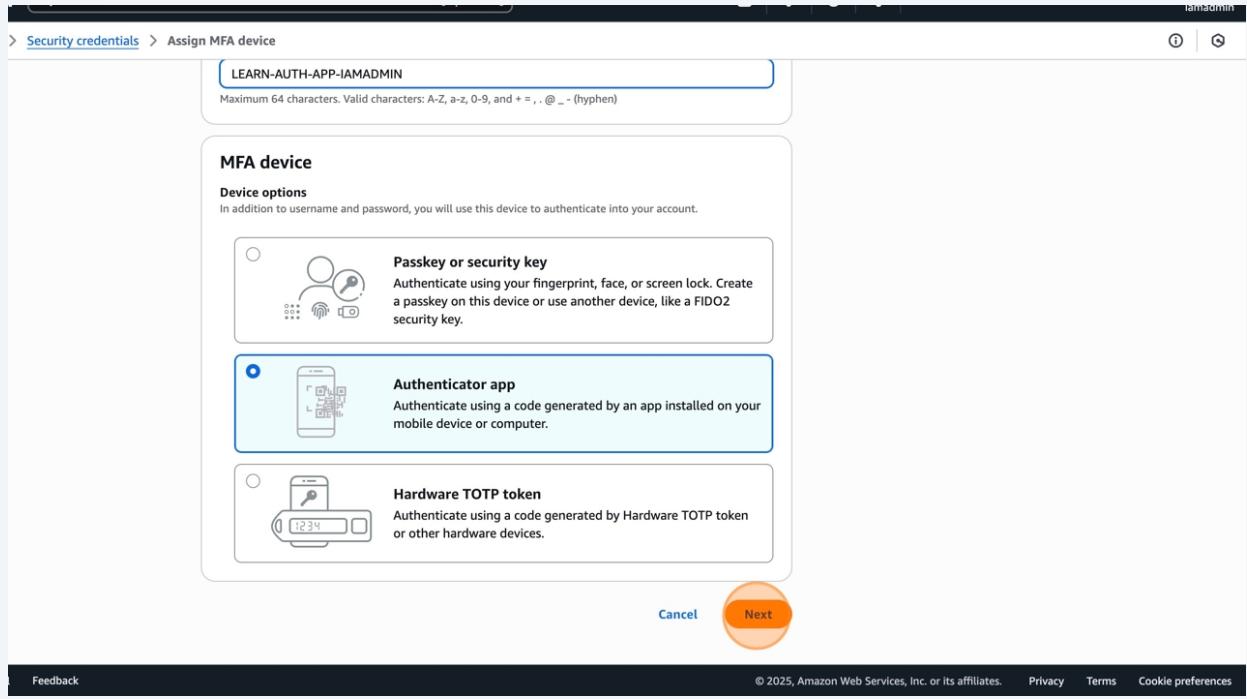
24

Click the "Device name" field and choose a name for your device. I chose "LEARN-AUTH-APP-IAMADMIN".



25

Select the "Authenticator app" option and click on "Next".



26

Click "Show QR code" and scan the code with your authenticator app and you will be presented with an MFA code that constantly changes. Typically about 30 seconds apart.

Step 1
● Select MFA device
Step 2
● Set up device

Set up device Info

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3 Type two consecutive MFA codes below
Enter a code from your virtual app below

Wait 30 seconds, and enter a second code entry.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookies

27

Click the "Enter a code from your virtual app below" field and enter the MFA code provided.

Step 1
● Select MFA device
Step 2
● Set up device

Set up device Info

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

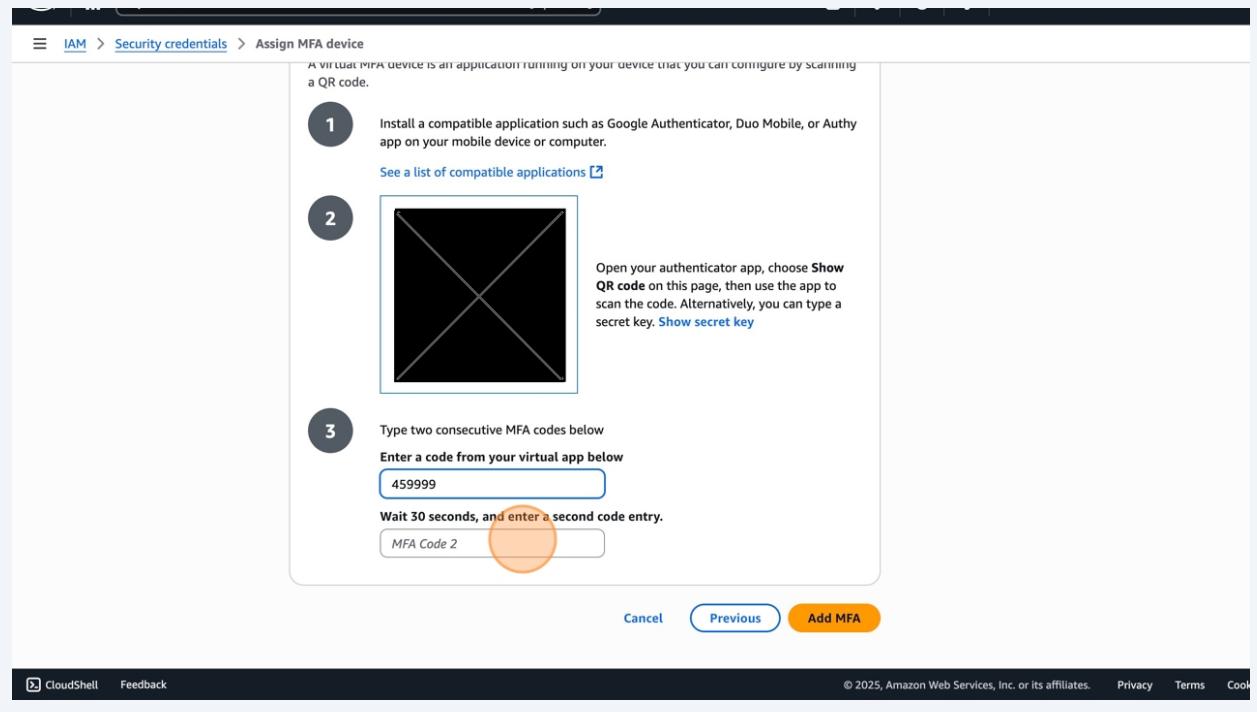
1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3 Type two consecutive MFA codes below
Enter a code from your virtual app below
 MFA Code 1
Wait 30 seconds, and enter a second code entry.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookies

28 Click the "Wait 30 seconds, and enter a second code entry." field.

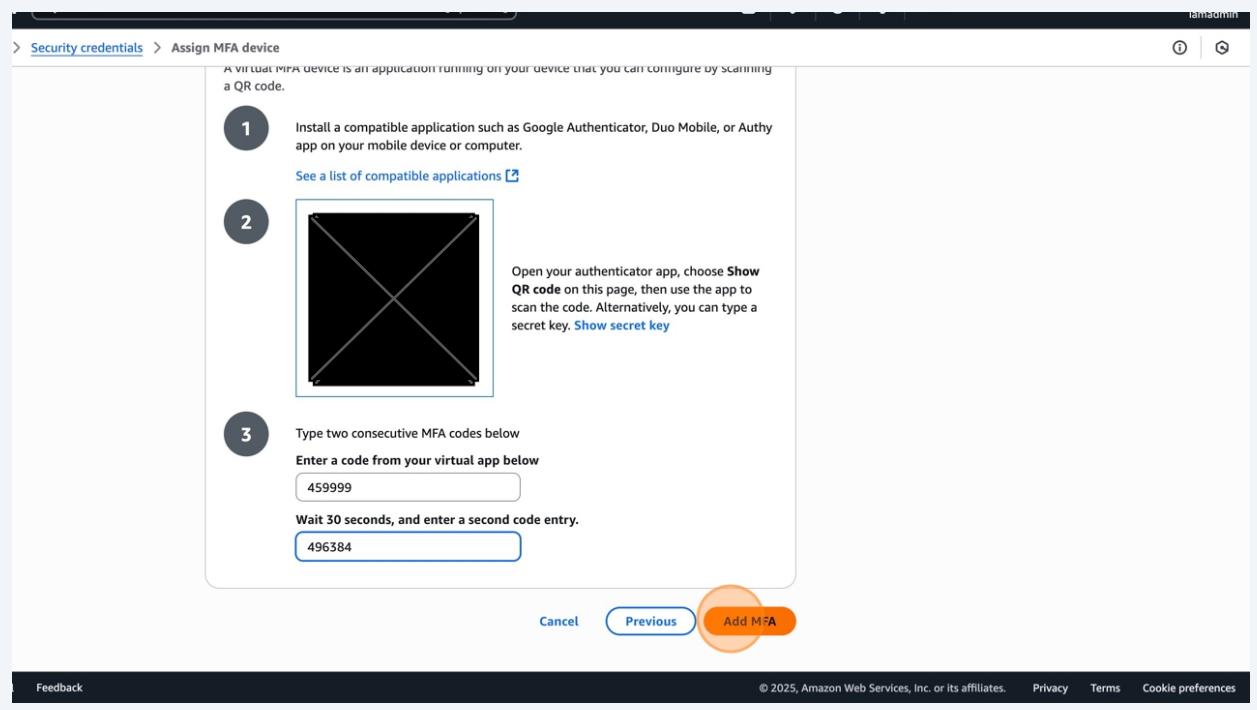


A screenshot of the AWS IAM 'Assign MFA device' wizard, Step 3. The page title is 'Assign MFA device'. The main content area contains three steps:

1. A QR code for a virtual MFA device.
2. A placeholder for a QR code from an authenticator app.
3. A text input field labeled 'Enter a code from your virtual app below' containing '459999', and a smaller field below it labeled 'Wait 30 seconds, and enter a second code entry.' containing 'MFA Code 2'.

The 'Wait 30 seconds, and enter a second code entry.' field is highlighted with an orange circle. At the bottom are 'Cancel', 'Previous', and 'Add MFA' buttons.

29 Click "Add MFA"



A screenshot of the AWS IAM 'Assign MFA device' wizard, Step 3. The page title is 'Assign MFA device'. The main content area contains three steps:

1. A QR code for a virtual MFA device.
2. A placeholder for a QR code from an authenticator app.
3. A text input field labeled 'Enter a code from your virtual app below' containing '459999', and a smaller field below it labeled 'Wait 30 seconds, and enter a second code entry.' containing '496384'.

The 'Add MFA' button at the bottom right is highlighted with an orange circle. At the bottom are 'Cancel', 'Previous', and 'Add MFA' buttons.

30

And that's it! Now Let's log out to test if the process has been completed. Click on the account dropdown. Copy the "Sign-in URL"

The screenshot shows the AWS IAM Security Credentials page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main content area is titled 'My security credentials' and contains 'Account details' for the user 'iamadmin'. It shows the User ARN (arn:aws:iam::170928836744:user/iamadmin) and Canonical user ID (ac4bbc0ee63097d8b9dd4e1187199997241e3496097ca38322b53ea99). Below this, there are tabs for 'AWS IAM credentials' (selected), 'AWS CodeCommit credentials', 'Amazon Keypairs credentials', and 'Amazon Bedrock API keys'. Under the 'AWS IAM credentials' tab, there's a section for 'Console sign-in' with a 'Console sign-in link' (https://canks-learning-aws-general.signin.aws.amazon.com/console) which is circled in orange. To the right of this, there are sections for 'Console password' (updated 5 minutes ago) and 'Last console sign-in' (3 minutes ago). At the bottom right of the page, there are links for 'CloudShell', 'Feedback', and 'Privacy Terms Cookies'.

31

Click on the account dropdown.

The screenshot shows the same AWS IAM Security Credentials page as the previous one, but with a different focus. The account dropdown in the top right corner is circled in orange. A tooltip message 'Console sign-in link copied' appears near the bottom left of the page, indicating that the sign-in URL has been copied to the clipboard. The rest of the interface is identical to the first screenshot.

32 Click "Sign out"

The screenshot shows the AWS IAM Security Credentials page. On the right side, there's a sidebar with account information: Account ID (170928836744), IAM user (iamadmin). Below that are links for Account, Organization, Service Quotas, Billing and Cost Management, and Security credentials. At the bottom of the sidebar are three buttons: 'Turn on multi-session support', 'Switch role', and 'Sign out', with 'Sign out' being highlighted with an orange circle.

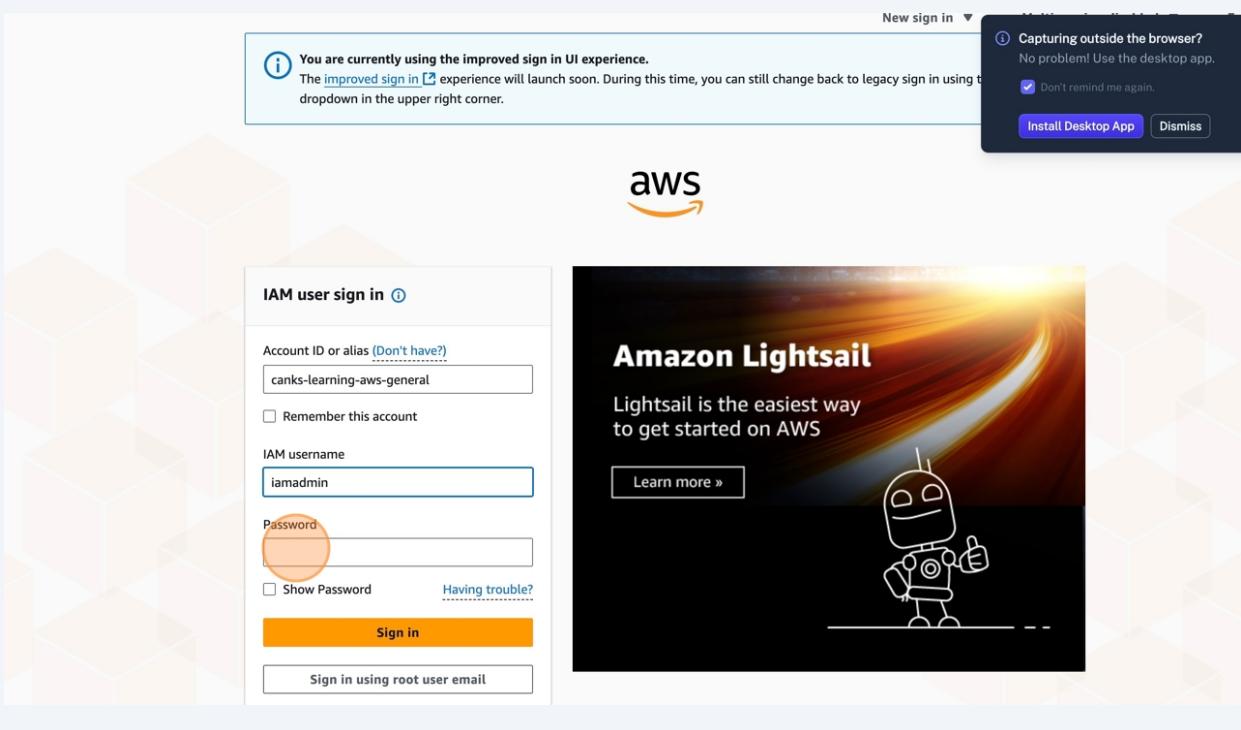
The main content area displays 'Account details' for the user iamadmin. It shows the User name (iamadmin), AWS account ID (170928836744), User ARN (arn:aws:iam::170928836744:user/iamadmin), and Canonical user ID (acb4bbc0ee63097d8b9dd4e118719999). Below this are tabs for AWS IAM credentials, AWS CodeCommit credentials, Amazon Keypairs credentials, and Amazon Bedrock API keys. Under the AWS IAM credentials tab, there's a 'Console sign-in' section with a 'Console sign-in link' (https://canks-learning-aws-general.signin.aws.amazon.com/console) and a 'Console password' (Updated 5 minutes ago). A note indicates that the improved sign-in experience will launch soon. At the bottom of the page are links for 'Feedback', '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

33 Navigate to a new tab and past the earlier copied "Sign-in URL".

The screenshot shows the AWS IAM user sign-in page. The 'IAM username' field is highlighted with an orange circle. The page also includes fields for 'Account ID or alias' (canks-learning-aws-general), 'Password', and 'Show Password'. There are checkboxes for 'Remember this account' and 'Having trouble?'. Below the form are 'Sign in' and 'Sign in using root user email' buttons. To the right of the sign-in form is a promotional banner for Amazon Lightsail, featuring a cartoon character and the text 'Amazon Lightsail' and 'Lightsail is the easiest way to get started on AWS'. At the top of the page, there's a message about the improved sign-in experience and a notification about capturing outside the browser.

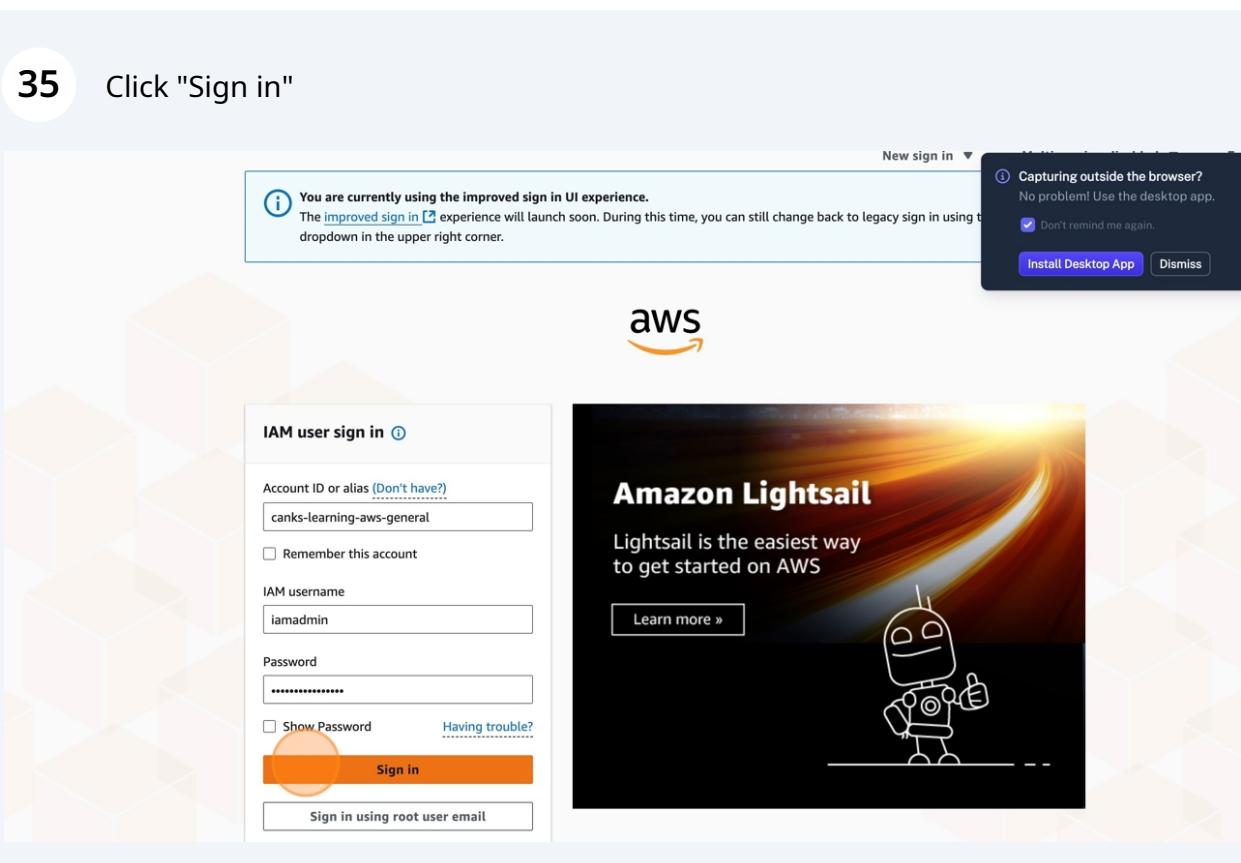
34

Fill in the "IAM username" and the "Password" field.



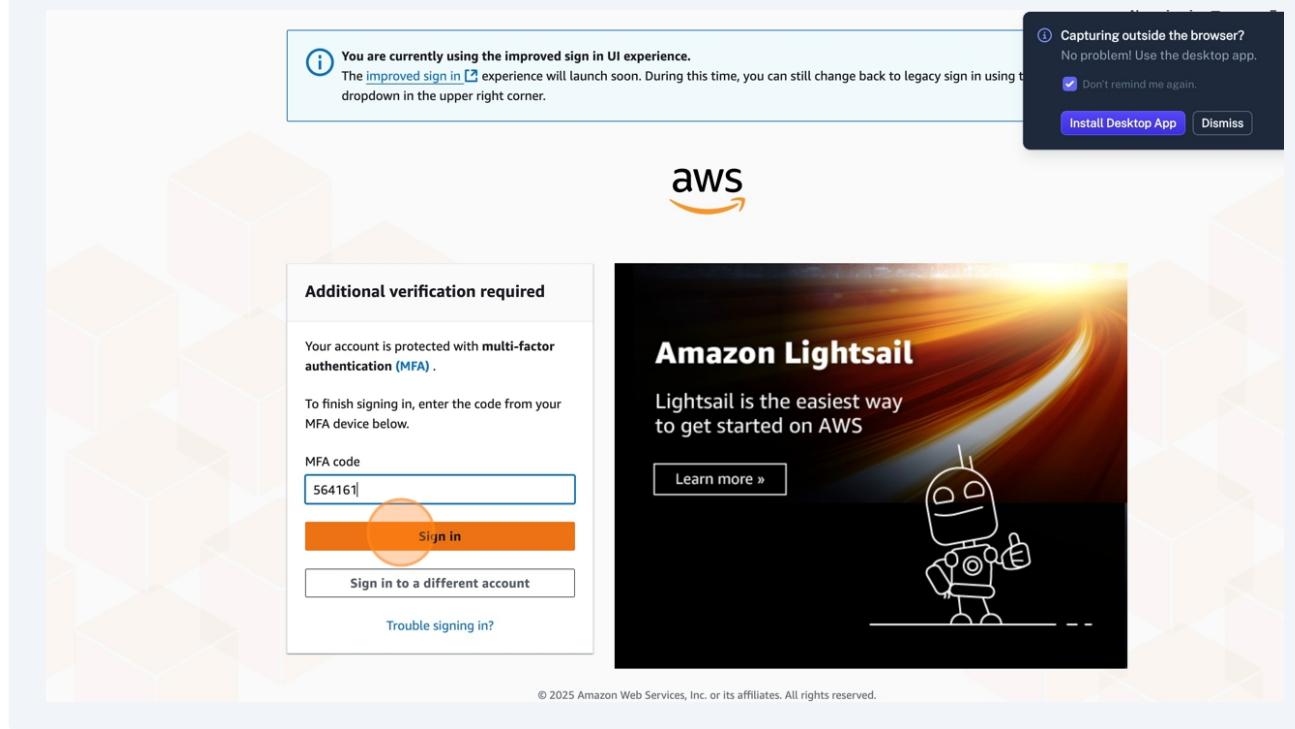
35

Click "Sign in"



36

You will be prompted to enter the MFA code for the MFA app. Enter the code and click "Sign in"..... If it works, You are done!



37

And...that's a wrap!

The screenshot shows the AWS Console Home page. The top navigation bar includes the AWS logo, a search bar, and a "Console Home" link. The main content area features several cards: "Recently visited" (IAM), "Welcome to AWS" (Getting started with AWS, Learn the fundamentals and find valuable information to), "AWS Health" (Open issues 0, Past 7 days), and "Cost and usage" (Current month \$26.78, Cost (\$), Forecasted month end 20). On the right, there's a section for "Applications (0)" with a "Create application" button and a "Go to myApplications" link. The bottom of the page has a "Reset to default layout" button and a "+ Add widgets" button.