

AWS ACCOUNT SETUP

Critical: Students must complete the following instructions before attempting any of the course lab exercises. Please ask for help right away if you need it! OnDemand students, please email online-sme@sans.org.

Objectives

Guide you through creating and securing your Amazon Web Services (AWS) account. The steps required to complete this activity include:

- Create an AWS account.
- Secure the AWS default root user.
- Create a new AWS user for course lab exercises.
- Fix IAM dashboard warnings
- Install VMware Workstation Player, Workstation Pro, or Fusion.

Prerequisites

To set up and secure your new AWS account, you will need the following:

- A web browser with access to AWS
- Credit card to set up AWS account
- A phone number to verify your account setup (AWS will call to finalize setup process)

Overview

Students will need access to their own Amazon Web Services (AWS) account to complete the lab exercises in the *SEC545: Cloud Security Architecture and Operations* course. These setup instructions will walk the student through initial AWS Account setup, configuring multi-factor authentication (MFA) for the root user account (a best practice), removing programmatic access from the root user, and creating a separate privileged account to use for lab exercises.

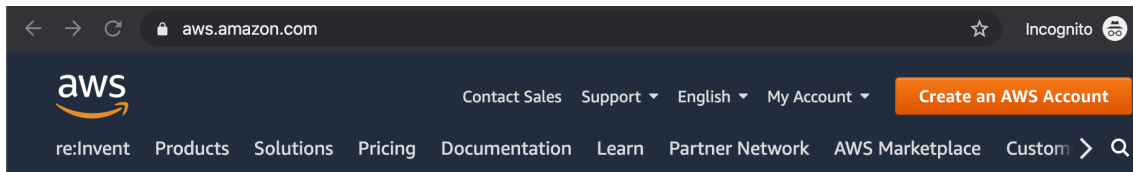
Attention: SANS strongly recommends students use a new AWS account for this course.

Create an AWS Account

Warning: We strongly recommend creating a new AWS account. Using an existing account may lead to networking conflicts and other problems in future labs. You can cancel the account at the end of the class if you want.

1. Navigate to <http://aws.amazon.com/> and click the button on the top right.

Note: The text on the button may be different. It could say "Sign up", "Create an Account", or "Sign In to the Console."



2. Follow the instructions to create a new account.

Note: If you see a login screen, click "Create a new AWS Account."



Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

username@example.com

Next

— New to AWS? —

Create a new AWS account


Otherwise you should see a screen such as the following right away:


aws English ▾


Create an AWS account


AWS Accounts Include 12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB
Visit aws.amazon.com/free for full offer terms

Email address 

Password 

Confirm password 

AWS account name 

[Continue](#)

[Sign in to an existing AWS account](#)

© 2020 Amazon Web Services, Inc. or its affiliates.
All rights reserved.
[Privacy Policy](#) | [Terms of Use](#)

Note: To complete the process, you will need to enter a credit card number and receive a phone call from Amazon to enter a code. It will ask you if you want to create a support plan. Just select the free, basic support plan to avoid additional charges. You will have to validate your account by responding to a phone call. If you are setting up an account outside the US, you may have additional steps provided to you by Amazon.

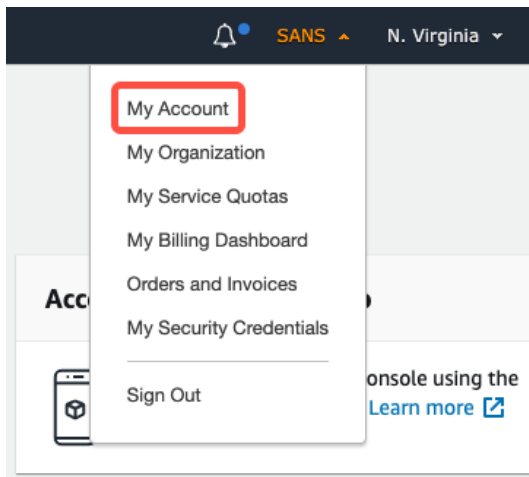
Best practice: When setting up a new AWS account for an organization, use an alias that will remain valid even if the person setting up the account leaves the company. For example, for an account set up for the pen testing division of Voodoo Security, the alias might be `aws-pentesting@voodoosec.com` and emails might go to the person in charge of the pen testing division, CIO, and a person responsible for AWS billing. For now, just use any email you want.

Tip: If you start your email aliases with "aws" they will follow the instructions on each screen until you have successfully created an account.

After completing the account creation process, you will be redirected to the login screen.

3. Sign in to your new account by clicking "**Sign in to the Console**" at the top of the page.

Look at your billing information by clicking on the account name you selected. It will be on the right side of the black bar at the top of the screen. Click on "**My Account**."



This section shows where you would set up alternate billing contacts and create challenge questions.

▼ Alternate Contacts [Edit](#)

In order to keep the right people in the loop, you can add an alternate contact for Billing, Operations, and Security communications. To specify an alternate contact, click the Edit button.

Please note that, as the primary account holder, you will continue to receive all email communications.

Billing ⓘ

Contact: None

Operations ⓘ

Contact: None

Security ⓘ

Contact: None

▼ Configure Security Challenge Questions [Edit](#)

Improve the security of your AWS account by adding security challenge questions. We use these to help identify you as the owner of your AWS account if you ever need to contact our customer service for help.

Security questions are currently not enabled.

This section allows turning on or off access to billing for anyone but the root user in the account.

Large companies may want to consider using AWS Organizations and Consolidated Billing to segregate billing responsibilities into a separate account. For more information about organizations see: <https://aws.amazon.com/organizations/>

▼ IAM User and Role Access to Billing Information [Edit](#)

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).

IAM user/role access to billing information is deactivated.

This screen is also where companies can sign up for GovCloud if part of the US Government.

▼ GovCloud (US)

[Sign up for AWS GovCloud \(US\)](#)

Closing your AWS Account

1. Under the "My Account" screen, you can close the account. If you don't want to keep your AWS account or incur additional charges beyond those in class, this is where you would come.

▼ Close Account

☐ understand that by clicking this checkbox, I am closing my AWS account. The closure of my AWS account serves as notice to AWS that I wish to terminate the AWS Customer Agreement or any other agreement with AWS that governs my AWS account, solely with respect to that AWS account.

Monthly usage of certain AWS services is calculated and billed at the beginning of the following month. If I have used these types of services this month, then at the beginning of next month I will receive a bill for usage that occurred prior to termination of my account. In addition, if I have any active subscriptions (such as a Reserved Instance for which I have elected to pay in monthly installments), then even after my account is closed I may continue to be billed for the subscription until the subscription expires or is sold in accordance with the terms governing the subscription.

I acknowledge that I may reopen my AWS account only within 90 days of my account closure (the "Post-Closure Period"). If I reopen my account during the Post-Closure Period, I may be charged for any AWS services that were not terminated before I closed my account. If I reopen my AWS account, I agree that the same terms will govern my access to and use of AWS services through my reopened AWS account.

If I choose not to reopen my account after the Post-Closure Period, any content remaining in my AWS account will be deleted. For more information, please see the the [Amazon Web Services Account Closure page](#).

☐ understand that after the Post-Closure Period I will no longer be able to reopen my closed account.

☐ understand that after the Post-Closure Period I will no longer be able to access the Billing Console to download past bills and tax invoices.

If you wish to [download any statements you can do so here](#). Select the month and expand the summary section to download the payment invoices and/or tax documents.

☐ understand that after the Post-Closure Period I will not be able to create a new AWS account with the email address currently associated with this account.

If you wish to update your e-mail address, [follow the directions here](#).

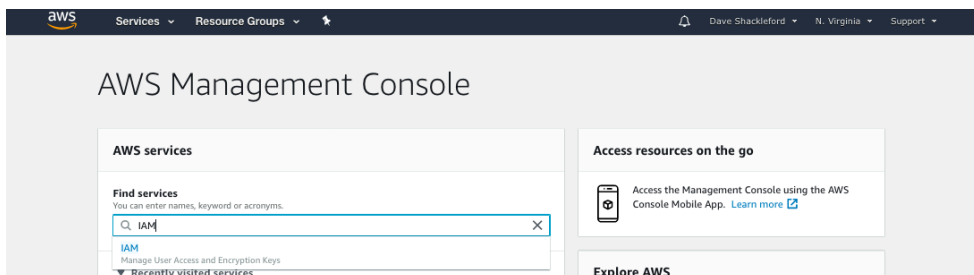
[Close Account](#)

Secure the Root User

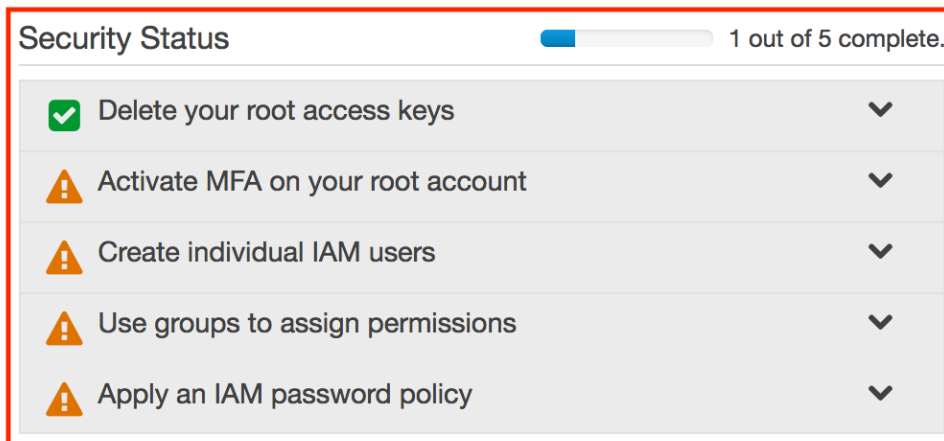
Best practice: AWS best practices include some immediate changes to protect the default root user. These protections are located under the IAM (Identity and Access Management) service in AWS, which allows you to manage access to AWS services in your account.

Remove API Access Keys

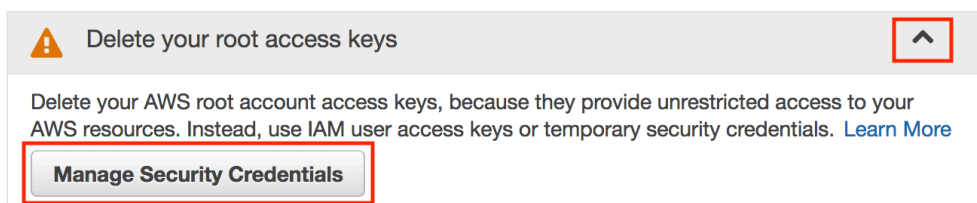
1. **Navigate to the IAM service.** First, click on the AWS logo. Type IAM in the search box and click IAM.



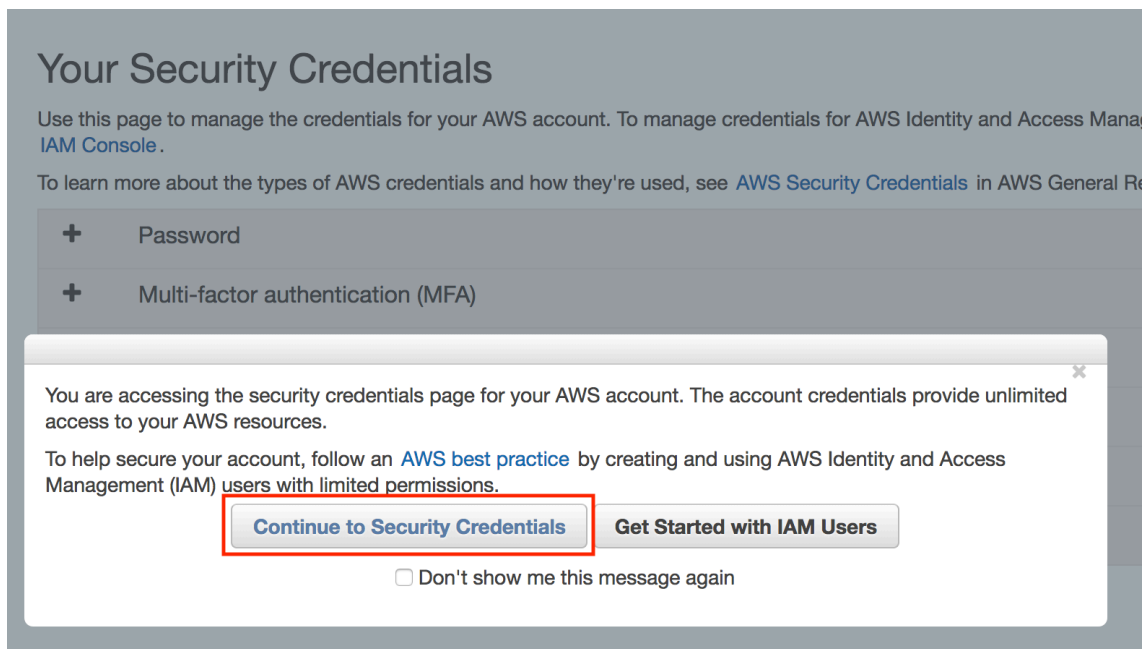
2. Verify there is a green checkbox next to "Delete your root access keys."



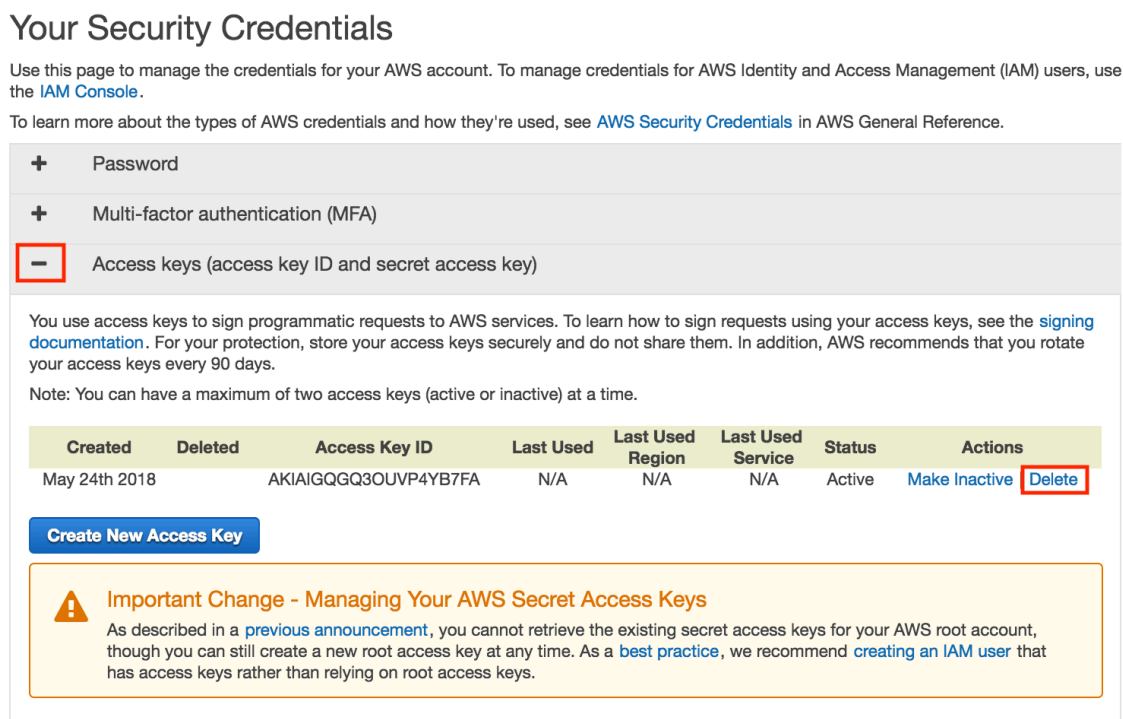
- a. If you see a yellow triangle, click on the down arrow and then click "Manage Security Credentials."



- b. Click on "Continue to Security Credentials."



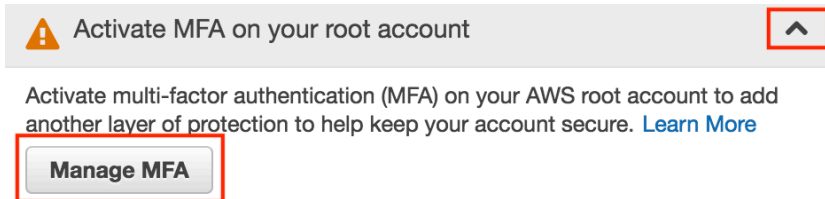
- c. Click the **plus sign (+)** next to **Access keys** and click **"Delete"** then the back arrow in your browser.



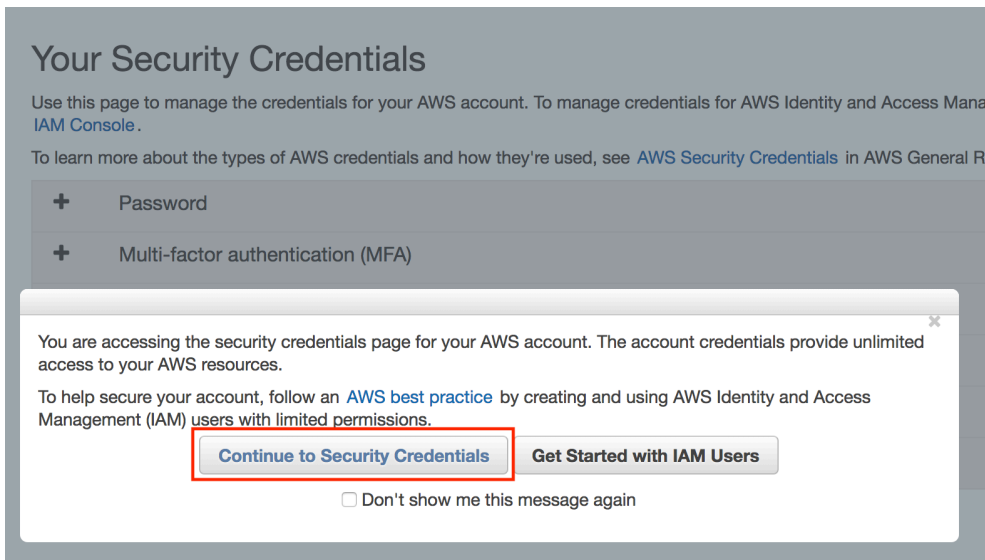
Now you should see the green checkbox as shown in step 2.

Set up MFA.

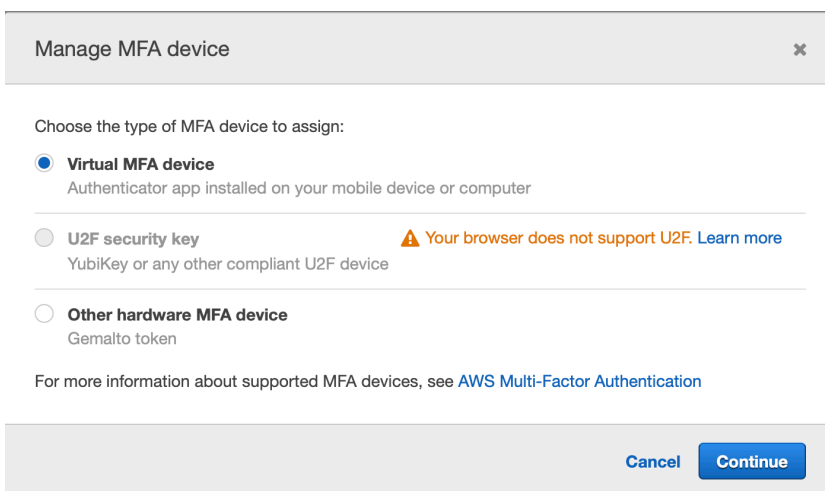
AWS security best practice includes setting up MFA (multifactor authentication) on your root account. The root account can cancel your account, change the contract information, and delete resources from your account. It is important to set up MFA (multifactor authentication) on this and any other user in your account that has a great deal of administrative access. Click the down arrow next to "Activate MFA on your root account," click "Manage MFA," and follow the instructions.



1. Click on "Continue to Security Credentials."



Choose "Virtual MFA device" (your cell phone) and click Continue.



2. You will now set up your virtual MFA device:

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer
See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code

Show QR code

Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

MFA code 2

Cancel

Previous

Assign MFA

Follow the link under Step 1 to set up an application on your phone to use for MFA. Scroll to the middle of the page and choose an application that works with your device. Follow the instructions to install the application on your device.

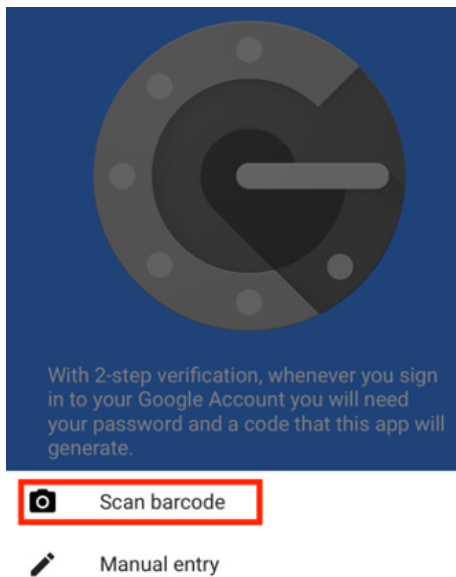
Note: [Google Authenticator](#) is likely the most popular choice at the time of this writing. Usually it's just a matter of going to the app store on your device, searching for "Google Authenticator," and choosing to install it.

Virtual MFA Applications

Applications for your smartphone can be installed from the application store that | applications for different smartphone types.

Android	Google Authenticator ; Authy 2-Factor Authentication
iPhone	Google Authenticator ; Authy 2-Factor Authentication
Windows Phone	Authenticator

3. Scan the QR Code to add your AWS account to the authenticator app.



4. Enter the numeric code from the authenticator into the AWS Console. Then wait for a new code to appear in the authenticator. Enter the second code. Then click "Assign MFA."

Critical: Protect this QR code. Anyone with access the QR code can add it to their own authenticator application.

Tip: Companies using virtual MFA to protect their root account should print out the QR code, store it in a safe or safety deposit box, and implement a two-person access control policy.

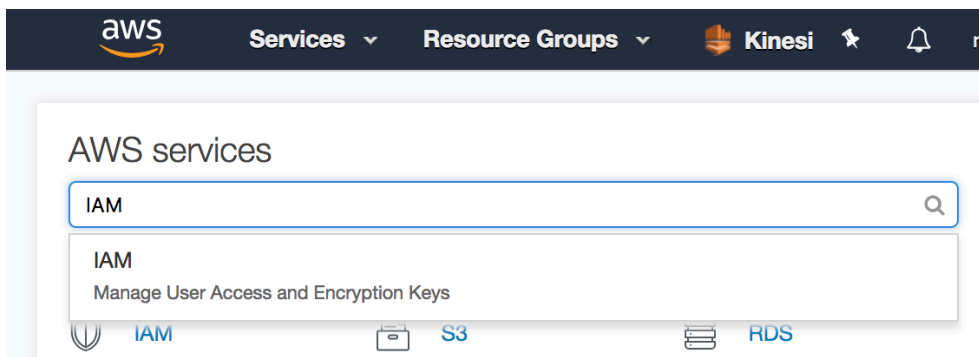
At this point, you have added MFA to your root account. From now on, you'll need to enter the code from the authenticator application on your phone to log in to your account.

Create an AWS User

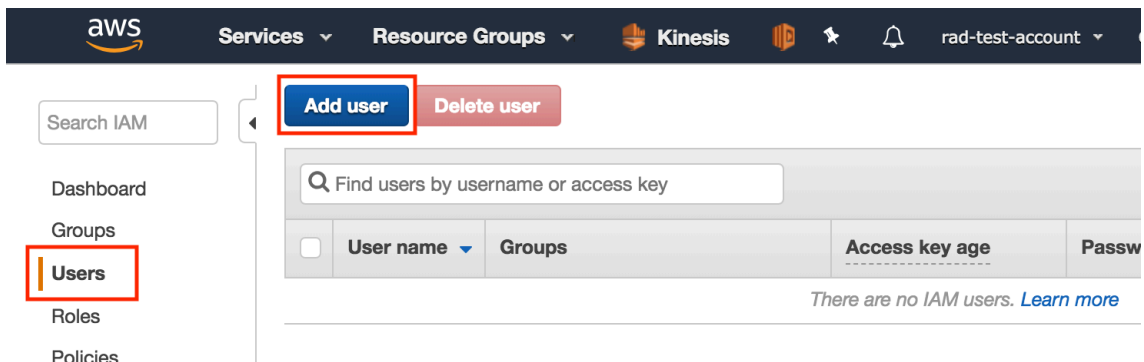
Best practice: For AWS IAM include not using the root account but instead setting up a new user and then using separate user accounts for normal operations. Lock away the root account access in a safe manner. *SANS SEC401 Security Bootcamp* discusses various mechanisms for securely storing sensitive, high-risk credentials.

1. **Navigate to the IAM** page in the AWS Console.

Click on the AWS logo. Type IAM in the search box.



2. Click on **"Users"** on the left and then click **"Add user"** at the top of the screen.



Add a new user with the following settings and click "**Next: Permissions**".

Note: Name of the user is **SEC545**. This is the user account you will be using in the course labs to perform actions in your AWS account. Change *YourPasswordHere* to a password you can remember. Also, be sure a checkmark appears besides "**AWS Management Console access**" and the **other checkboxes are empty**.

Add user

1

2

3

4

5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

SEC545

+

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

☐

Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

☐Autogenerated password

☒Custom password

YourPasswordHere

☒Show password

Require password reset

☐User must create a new password at next sign-in

* Required

Cancel

Next: Permissions

3. On the next screen, choose the last box, "Attach existing policies directly", then select "AdministratorAccess", and finally click "Next: Tags."

Note: The course covers policies in more detail.

Add user 1 2 3 4 5

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly 1

Create policy

Filter policies ▼ Showing 517 results

	Policy name ▼	Type	Used as
<input checked="" type="checkbox"/> 2	AdministratorAccess	Job function	Permissions policy (3)
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	None
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS managed	None

3

Cancel Previous **Next: Tags**

4. Click "Next: Review", click "Create user", and then click "Close."

Add user 1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Cancel Previous **Next: Review**

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	SEC545
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess

Tags

No tags were added.

Cancel

Previous

Create user

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

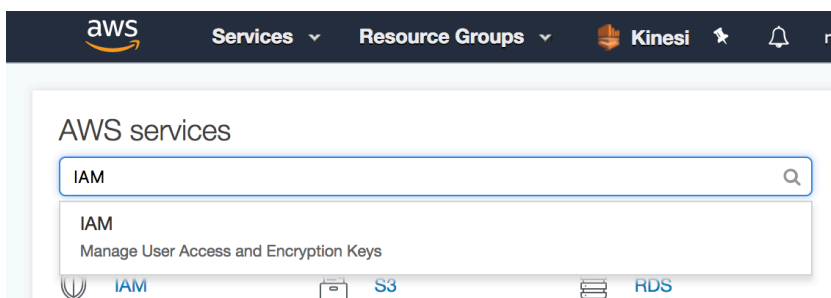
Users with AWS Management Console access can sign-in at: [https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console)

Download .csv

User	Email login instructions
SEC545	Send email

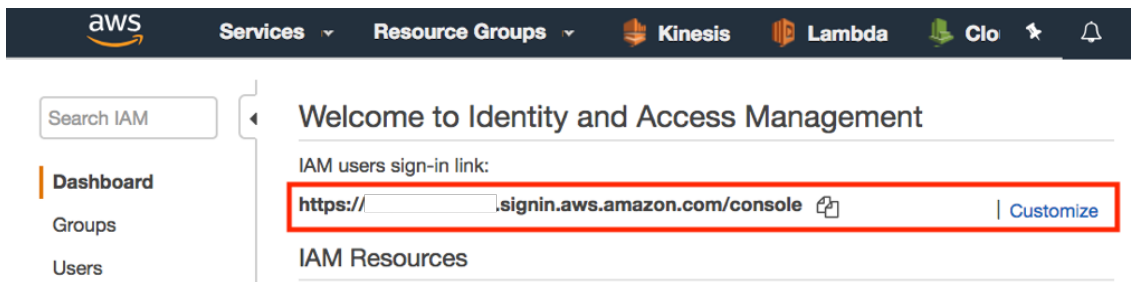
Close

Navigate to the IAM service. Click the AWS logo, search for IAM, and click on IAM.

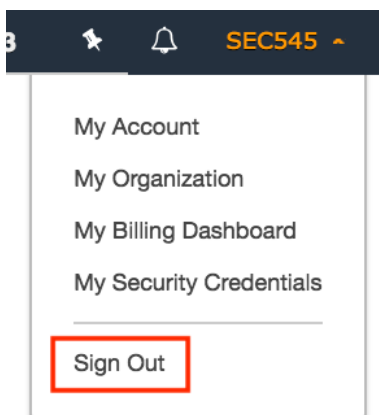


5. Copy the IAM users sign-in link as you will log in as the new user. *Customize it if you want.*

Hint: You might want to create a bookmark for this link!



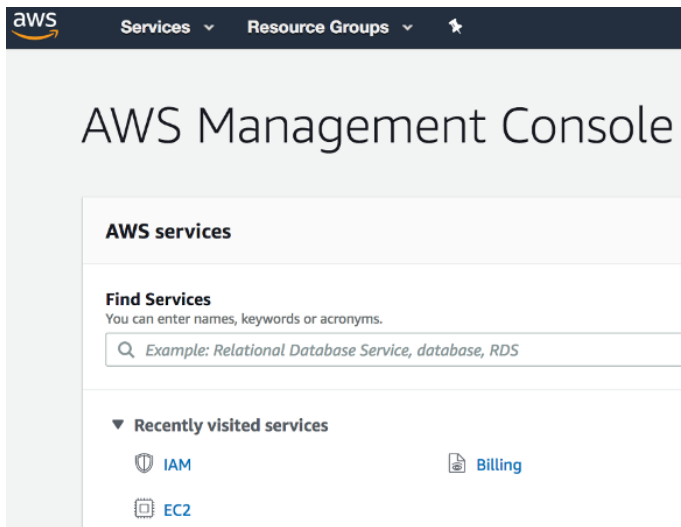
6. Sign out of your AWS account.



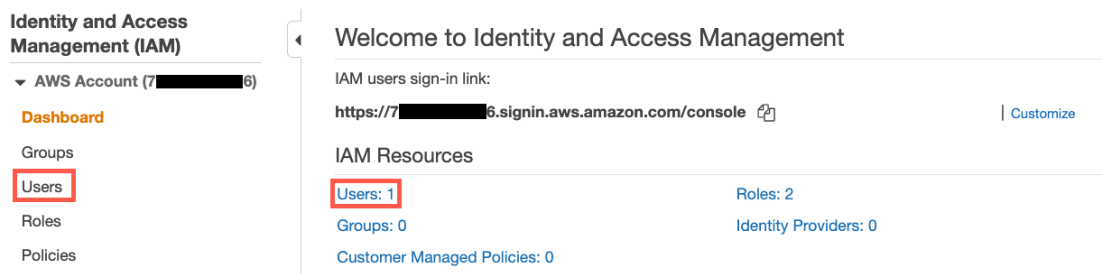
7. Sign in to your AWS account at the URL in Step 5 with the new user credentials.

A screenshot of the AWS sign-in page. At the top is the AWS logo. Below it are three input fields: 'Account ID or alias' with the value 'sec545-2sl', 'IAM user name' with the value 'SEC545', and 'Password' which is masked with dots. A blue 'Sign In' button is positioned below the password field. At the bottom, there is a link that reads 'Sign-in using root account credentials'.

8. Navigate to the IAM service by searching for it or clicking the IAM icon.

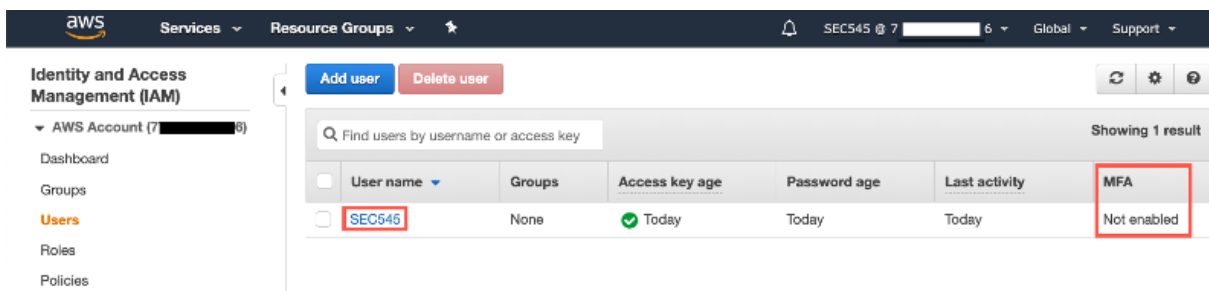


9. Click on Users on the left or in the middle of IAM Dashboard.



10. Click on the username to edit the user.

Note: MFA is not enabled.



11. Click the **Security Credentials** tab. Click "**Manage**" next to **Assigned MFA device**.

Follow the instructions to set up MFA. The process to add an MFA device to this user will be the same as adding MFA to the root account **as we did in Secure the Root User**.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with options like Dashboard, Groups, Users, Roles, Policies, etc. The main content area is titled 'Summary' for user 'SEC545'. It displays metadata such as User ARN, Path, and Creation time. Below this is a tabbed interface with 'Security credentials' selected. Under the 'Sign-in credentials' section, there are three rows: 'Summary' with a console sign-in link, 'Console password' which is enabled, and 'Assigned MFA device' which is 'Not assigned'. The 'Assigned MFA device' row has a 'Manage' link next to it. The 'Security credentials' tab and the 'Assigned MFA device' row are highlighted with red boxes.

Sign-in credentials	
Summary	• Console sign-in link: https://7[redacted]6.signin.aws.amazon.com/console
Console password	Enabled (last signed in Today) Manage
Assigned MFA device	Not assigned Manage
Signing certificates	None ✎

Fixing the IAM Dashboard Warnings

Add a Group

1. Navigate to the IAM service. Note we have two security warnings remaining.

Security Status 3 out of 5 complete.

✓	Activate MFA on your root account	▼
✓	Create individual IAM users	▼
⚠	Use groups to assign permissions	▼
⚠	Apply an IAM password policy	▼
✓	Rotate your access keys	▼

2. Click Groups on the left menu or in the center of the screen.

aws Services ▼ Resource Groups ▼

Identity and Access Management (IAM)

▼ AWS Account (xxxxxxxxxxxx)

Dashboard

Groups

Users

Roles

Policies

Welcome to Identity and Access Management

IAM users sign-in link:
<https://sans.signin.aws.amazon.com/console> | [Customize](#)

IAM Resources

Users: 0 Roles: 2

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

3. Click the "Create New Group" button.

aws Services ▼ Resource Groups ▼

Identity and Access Management (IAM)

▼ AWS Account (xxxxxxxxxxxx)

Dashboard

Groups

Users

Roles

Policies

Create New Group Group Actions ▼

Search

<input type="checkbox"/>	Group Name ↕	User
No records found.		

4. Enter group name "Sec545admin" and click "Next Step".

The screenshot shows the 'Set Group Name' step of the 'Create New Group Wizard'. The left sidebar lists the steps: 'Step 1 : Group Name', 'Step 2 : Attach Policy', and 'Step 3 : Review'. The main content area has the title 'Set Group Name' and a subtitle 'Specify a group name. Group names can be edited any time.' Below this is a text input field labeled 'Group Name:' containing the text 'Sec545admin'. A red box highlights the input field. Below the input field, there is a small example text: 'Example: Developers or ProjectAlpha' and 'Maximum 128 characters'. At the bottom right, there are two buttons: 'Cancel' and 'Next Step'. The 'Next Step' button is highlighted with a red box.

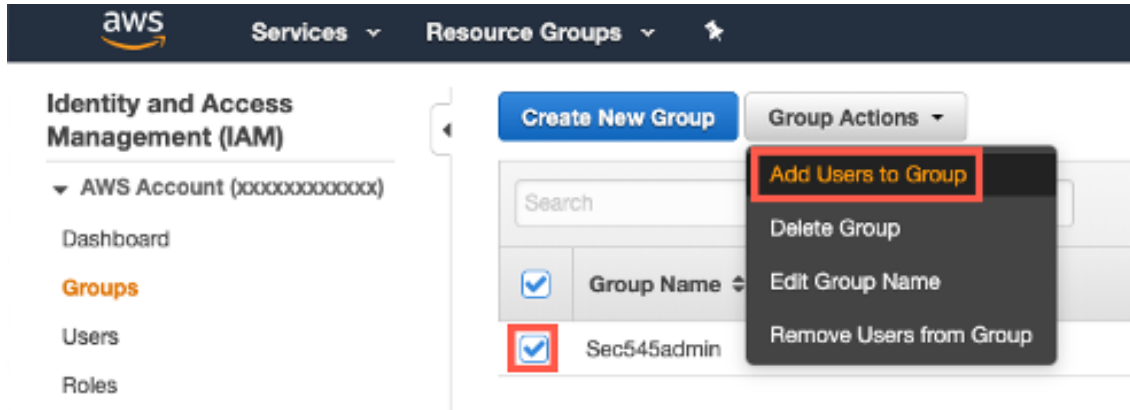
5. Select the "AdministratorAccess" policy and click "Next Step".

The screenshot shows the 'Attach Policy' step of the 'Create New Group Wizard'. The left sidebar lists the steps: 'Step 1 : Group Name', 'Step 2 : Attach Policy', and 'Step 3 : Review'. The main content area has the title 'Attach Policy' and a subtitle 'Select one or more policies to attach. Each group can have up to 10 policies attached.' Below this is a table with a filter 'Policy Type' and a search bar. The table shows 471 results. The first row is 'AdministratorAccess' with a checked checkbox (highlighted with a red box). The other rows are 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', and 'AlexaForBusinessCatalogFullAccess'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next Step'. The 'Next Step' button is highlighted with a red box.

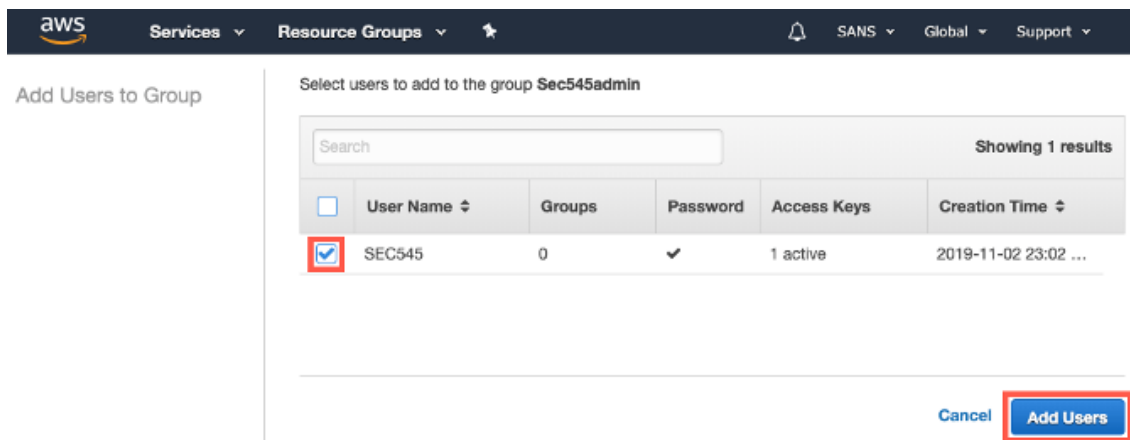
6. Review and click "Create Group."

The screenshot shows the 'Review' step of the 'Create New Group Wizard'. The left sidebar lists the steps: 'Step 1 : Group Name', 'Step 2 : Attach Policy', and 'Step 3 : Review'. The main content area has the title 'Review' and a subtitle 'Review the following information, then click **Create Group** to proceed.' Below this is a table with two rows: 'Group Name' with the value 'Sec545admin' and 'Policies' with the value 'arn:aws:iam::aws:policy/AdministratorAccess'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create Group'. The 'Create Group' button is highlighted with a red box.

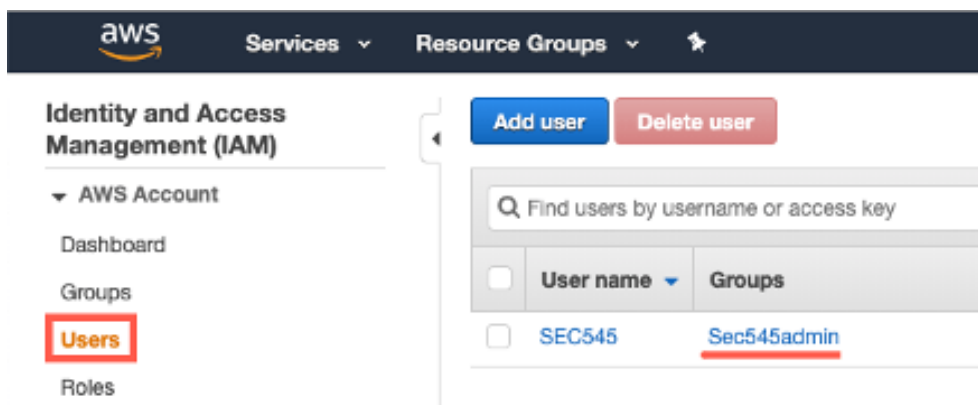
7. Select your group by checking the box next to it. Click "Group Actions" and "Add Users to Group."



8. Check the box next to the user we created, SEC545 and click "Add Users."



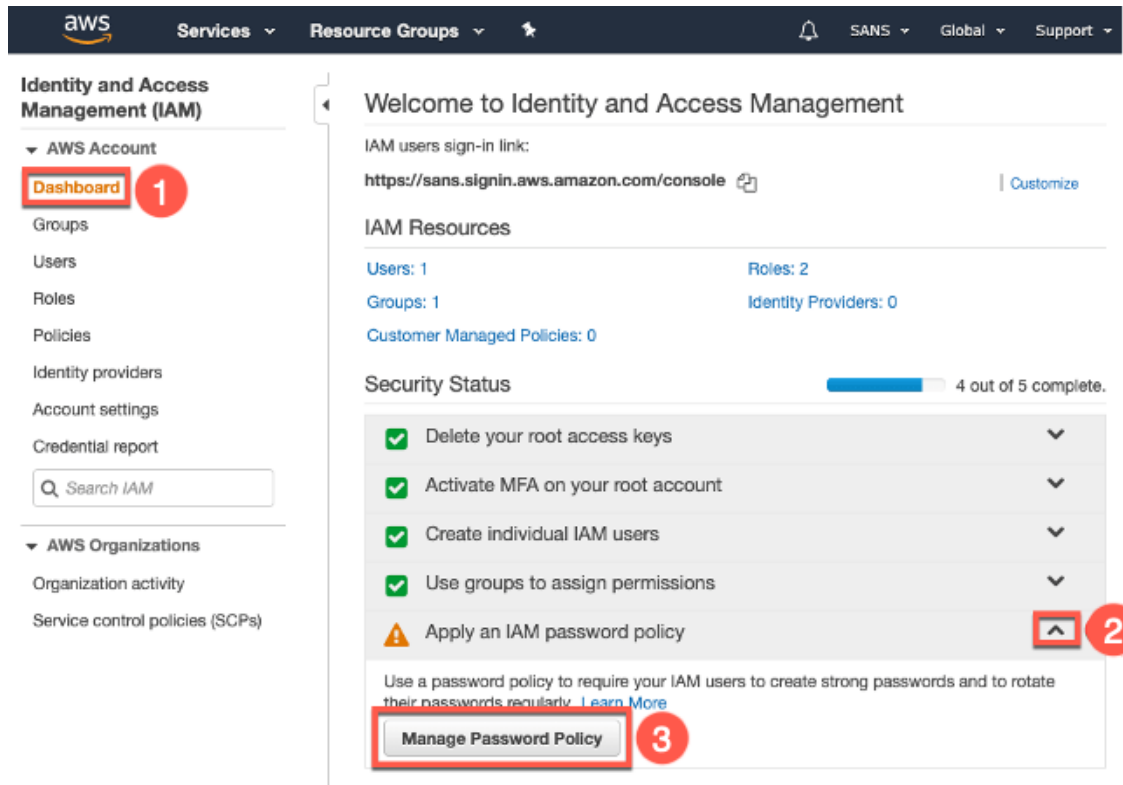
9. Click on Users in the left menu. Check that the "Groups" column for user "SEC545" says "Sec545admin."



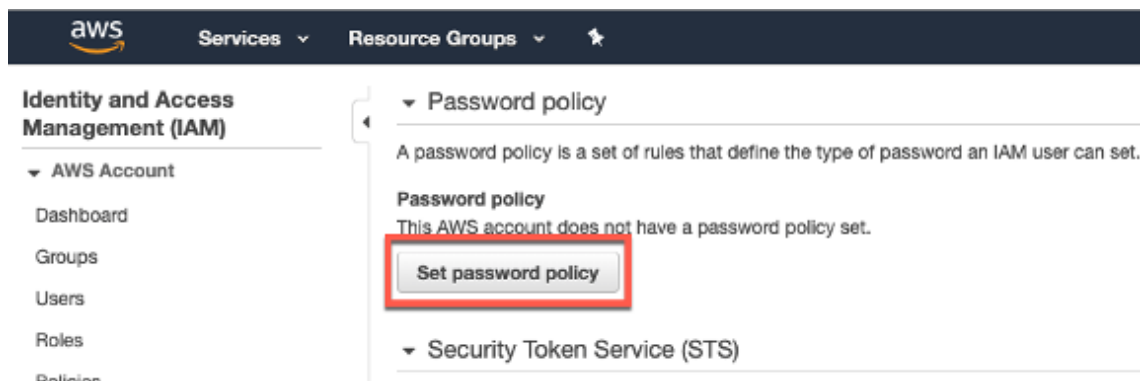
Set a Password Policy

1. Click "Dashboard" in the left menu, then the down arrow next to "Apply an IAM password policy", then click "Manage Password Policy."

Note: There is a yellow warning triangle and "!" indicating a security problem.



2. Click "Set password policy."



3. Enter a password policy and click "Apply password policy."

Choose your own password policy (possible sample shown below).

Note: Keep in mind this will be the required password strength for users you create in several additional labs, so we recommend setting a password policy that you can manage in class.

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

- ☒ Require at least one uppercase letter ⓘ
- ☒ Require at least one lowercase letter ⓘ
- ☒ Require at least one number ⓘ
- ☒ Require at least one non-alphanumeric character ⓘ
- ☒ Allow users to change their own password ⓘ
- ☒ Enable password expiration ⓘ
Password expiration period (in days):
- ☒ Prevent password reuse ⓘ
Number of passwords to remember:
- ☐ Password expiration requires administrator reset ⓘ

Apply password policy

Delete password policy

4. Return to the IAM Dashboard, and the IAM security status now shows all green checkboxes.

The screenshot shows the AWS IAM Dashboard. The left sidebar contains the navigation menu with 'Identity and Access Management (IAM)' selected. The main content area displays the 'Welcome to Identity and Access Management' page. The 'Security Status' section shows a progress bar at '5 out of 5 complete' and a list of five items, all of which are checked with green checkmarks:

- ✓ Delete your root access keys
- ✓ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy

VMware Installation & SEC545 VM Information

VMware Installation

1. **Install VMware Player or VMware Fusion** if you don't have it already installed on your system.

You can run virtual machines with the VMware software of your choosing if you already have something installed for this purpose. If not, please download and install.

VMware Player for Linux or Windows:

<https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html>

Download and install VMware Fusion for Mac:

<https://www.vmware.com/products/fusion/fusion-evaluation.html>

SEC545 Virtual Machine Information

The details for the SANS SEC545 VMs are as follows:

SEC545-CentOS VM

File: **SEC545-CentOS/SEC545-CentOS.vmx**

User: **student**

Password: **Passw0rd** *(with a zero, not a capital "o")*

IP Address: **10.10.10.10**

Elevating to root: **sudo su -**

XenServer VM

File: **XenServer/XenServer.vmx**

User: **root**

Password: **Passw0rd** *(with a zero, not a capital "o")*

IP Address: **10.10.10.30**