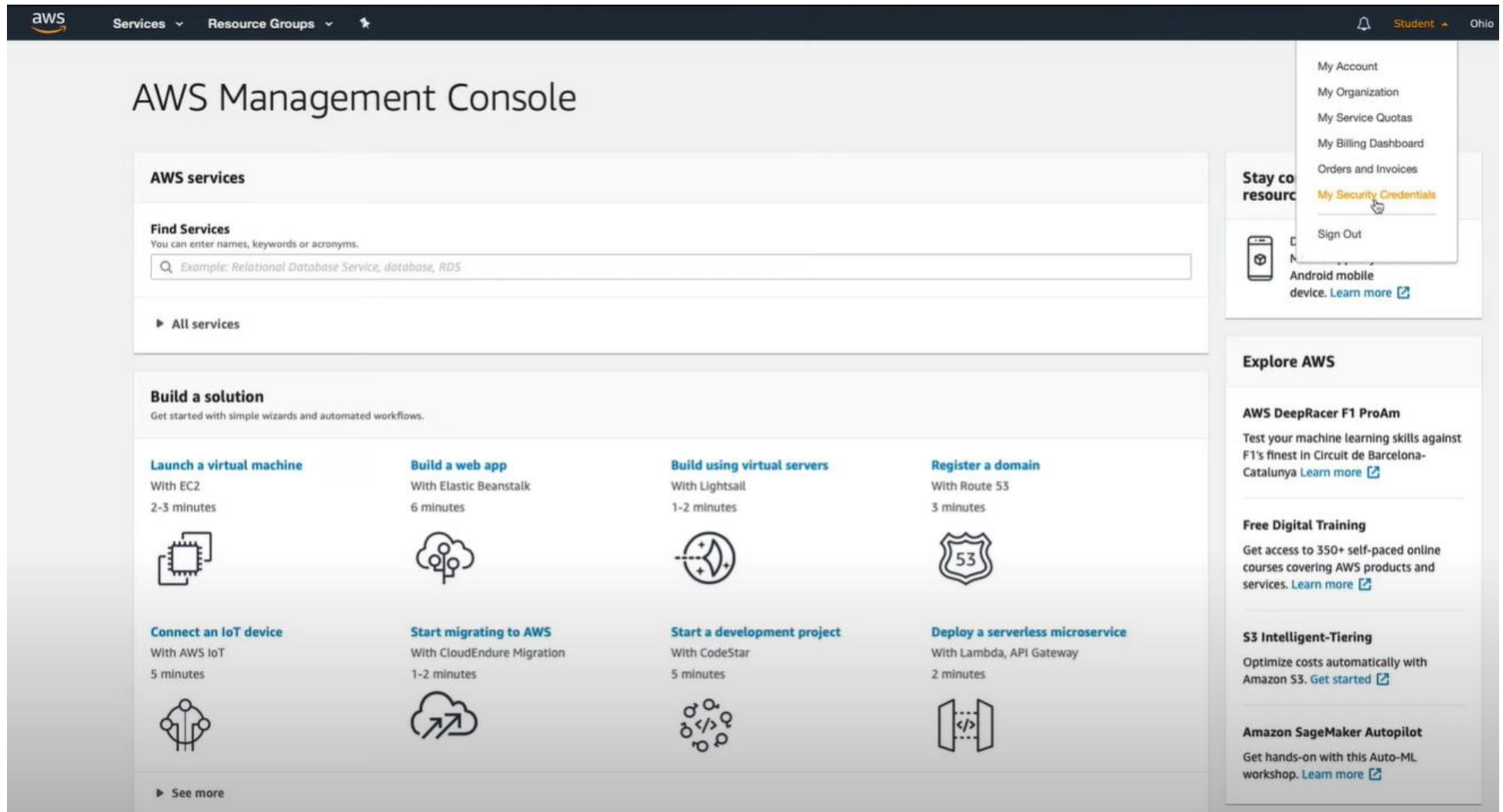


Securing Root User With MFA



The screenshot shows the AWS Management Console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a user profile dropdown. The user profile dropdown is open, showing options like 'My Account', 'My Organization', 'My Service Quotas', 'My Billing Dashboard', 'Orders and Invoices', 'My Security Credentials' (highlighted with a yellow bar and a mouse cursor), and 'Sign Out'. Below the navigation bar, the main content area is titled 'AWS Management Console'. It features a 'Find Services' search bar with the placeholder text 'Example: Relational Database Service, database, RDS'. Below the search bar, there are sections for 'AWS services', 'Build a solution' (with various guided solutions like 'Launch a virtual machine', 'Build a web app', etc.), and 'Explore AWS' (with featured services like 'AWS DeepRacer F1 ProAm', 'Free Digital Training', etc.).

Securing Root User With MFA

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a star icon. The left sidebar is titled 'Identity and Access Management (IAM)' and contains a 'Dashboard' section with links to 'Access management', 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. Below this is an 'Access reports' section with links to 'Access analyzer', 'Archive rules', 'Analyzers', 'Settings', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. At the bottom of the sidebar is a search bar labeled 'Search IAM' and the 'AWS account ID: 915464768551'. The main content area is titled 'Your Security Credentials' and includes instructions on how to manage credentials. It features a list of credential types: Password, Multi-factor authentication (MFA), Access keys (access key ID and secret access key), CloudFront key pairs, X.509 certificate, and Account identifiers. The 'Multi-factor authentication (MFA)' section is expanded, showing a description of MFA and a blue 'Activate MFA' button.

Identity and Access Management (IAM)

Dashboard

- Access management
 - Groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

Search IAM

AWS account ID:
915464768551

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

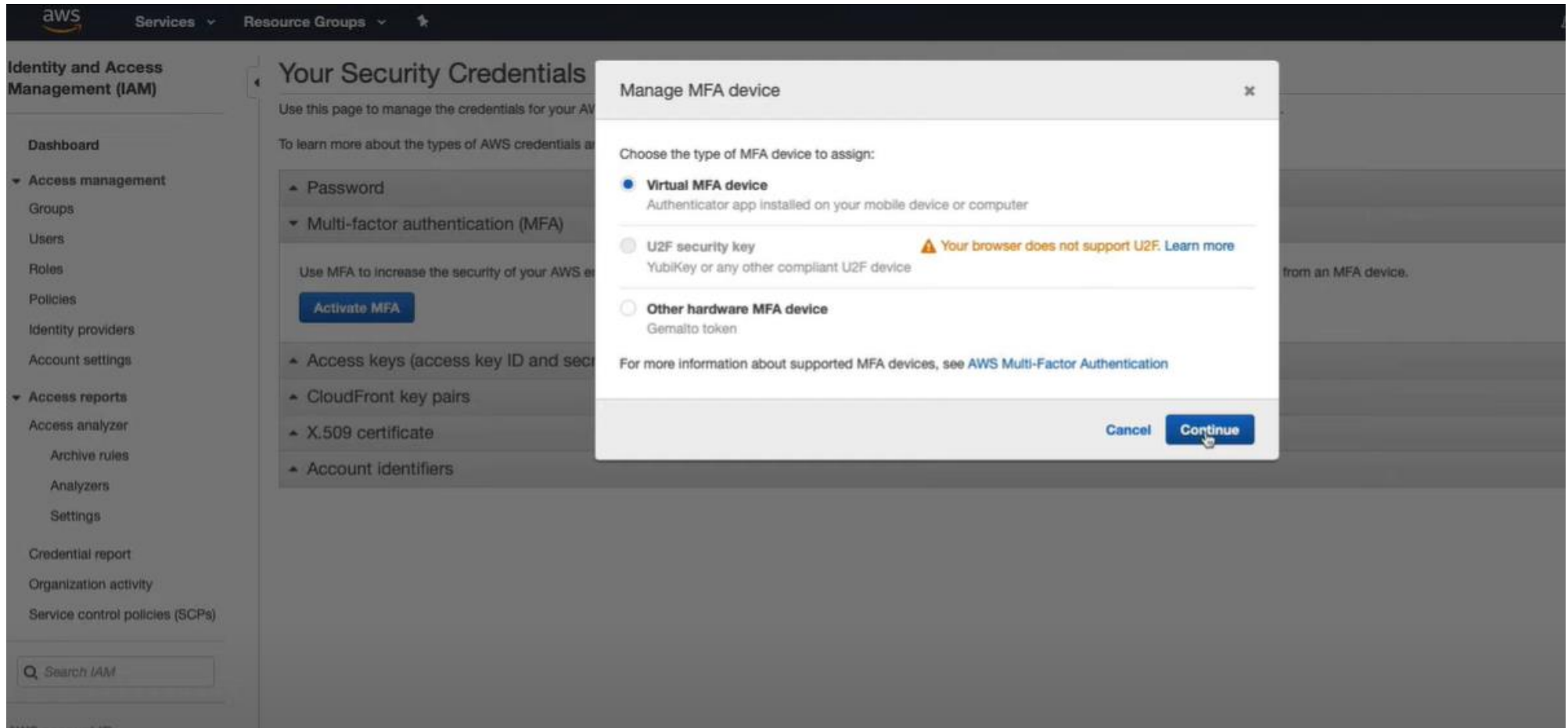
To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- ▲ Password
- ▼ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

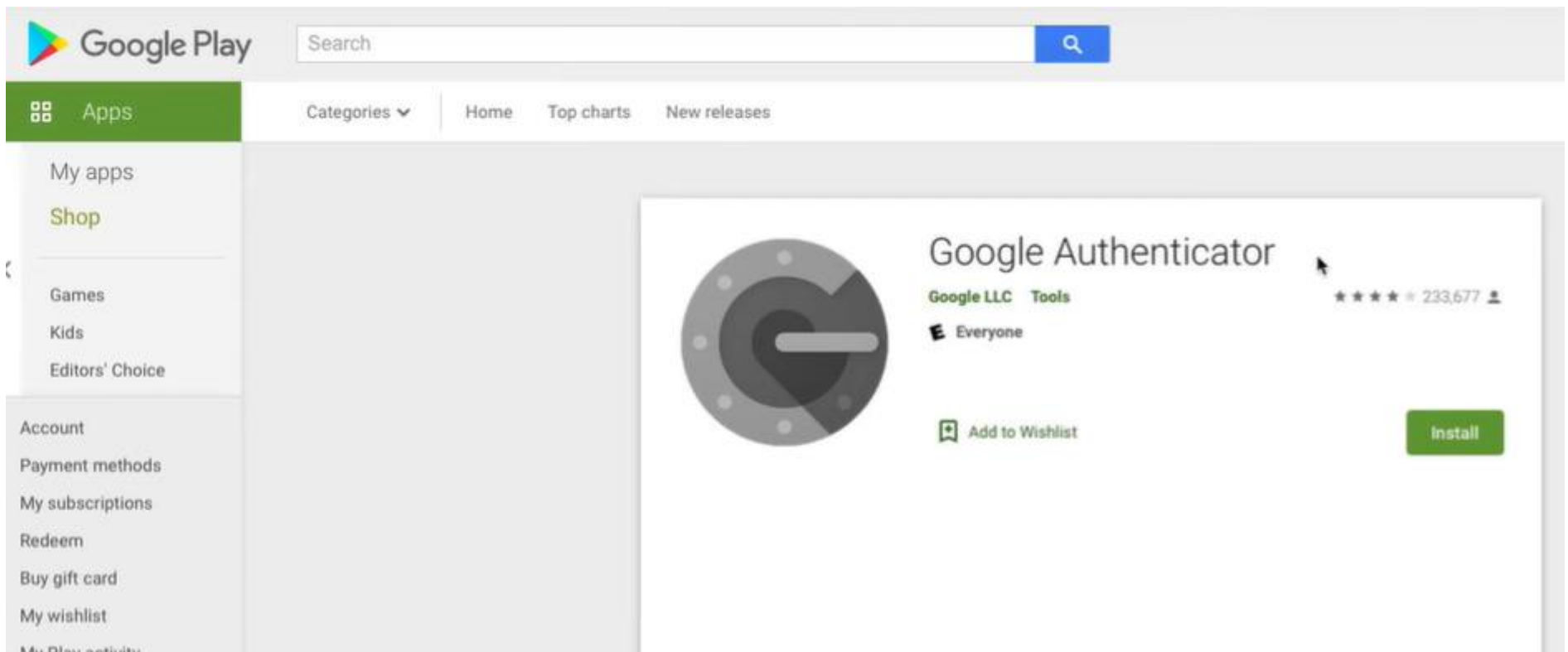
[Activate MFA](#)
- ▲ Access keys (access key ID and secret access key)
- ▲ CloudFront key pairs
- ▲ X.509 certificate
- ▲ Account identifiers

Securing Root User With MFA

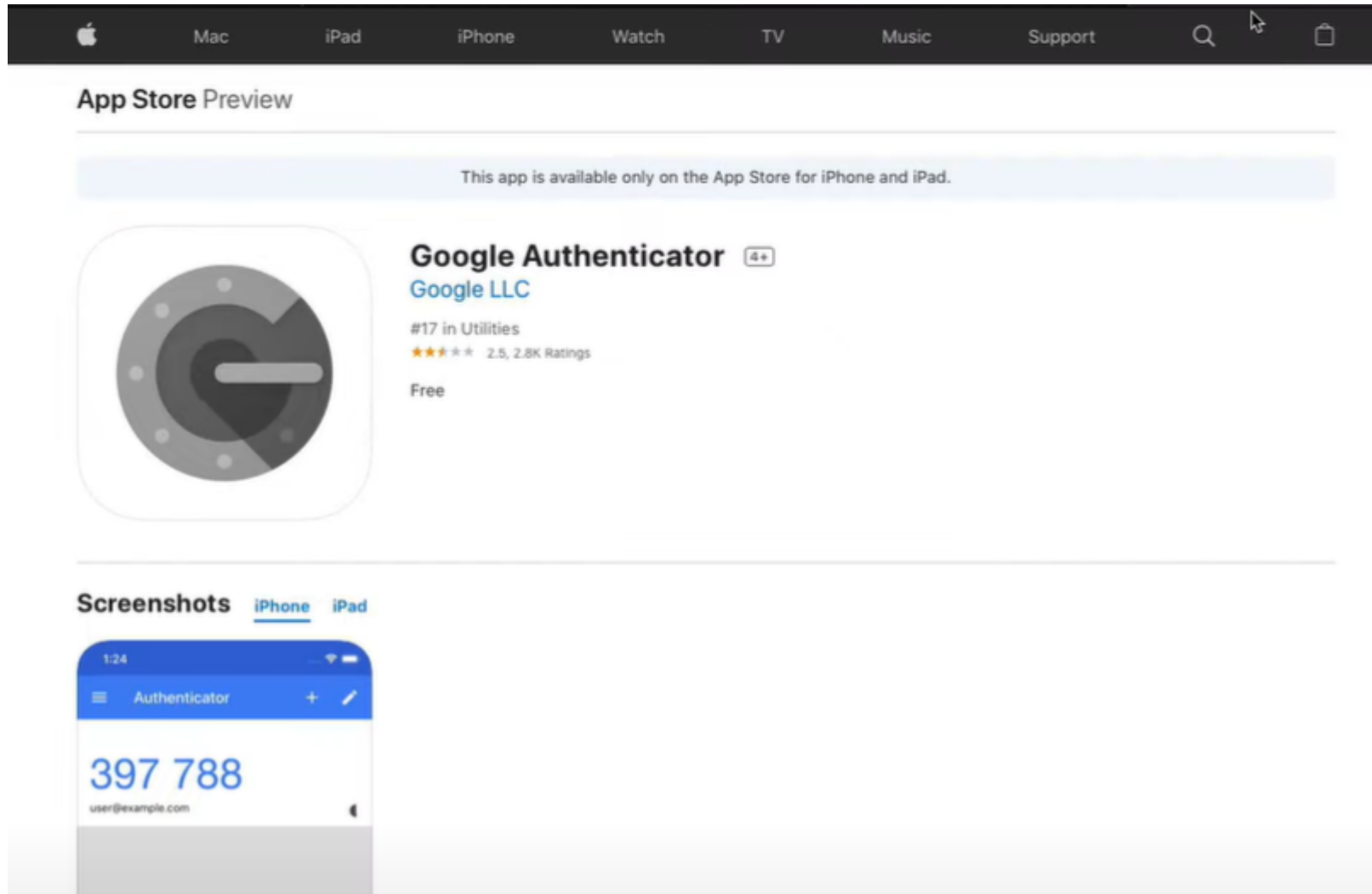


Securing Root User With MFA

Install Google Authenticator app.



Securing Root User With MFA



Securing Root User With MFA

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with a search bar and a list of navigation items including Dashboard, Access management, Groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SGPs). The main content area is titled 'Your Security Credentials' and lists various credential types: Password, Multi-factor authentication (MFA), Access keys, CloudFront key pairs, X.509 certificate, and Account identifiers. The 'Multi-factor authentication (MFA)' section is expanded, showing an 'Activate MFA' button. A modal dialog box titled 'Set up virtual MFA device' is open in the foreground. It contains three steps: 1. Install a compatible app on your mobile device or computer (with a link to 'See a list of compatible applications'), 2. Use your virtual MFA app and your device's camera to scan the QR code (with a 'Show QR code' button), and 3. Type two consecutive MFA codes below (with input fields for 'MFA code 1' and 'MFA code 2'). At the bottom of the dialog are 'Cancel', 'Previous', and 'Assign MFA' buttons. The background is dimmed to show the IAM console interface.

Securing Root User With MFA

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Access management' expanded. The main content area shows 'Your Security Credentials' with a list of credential types: Password, Multi-factor authentication (MFA), Access keys, CloudFront key pairs, X.509 certificate, and Account identifiers. The 'Multi-factor authentication (MFA)' section is selected, showing a description and an 'Activate MFA' button. A modal window titled 'Set up virtual MFA device' is open, guiding the user through three steps: 1. Install a compatible app, 2. Scan the QR code (which is displayed in a large box), and 3. Type two consecutive MFA codes. The first code is 640152 and the second is 736525. At the bottom of the modal, there are 'Cancel', 'Previous', and 'Assign MFA' buttons.

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
3. Type two consecutive MFA codes below

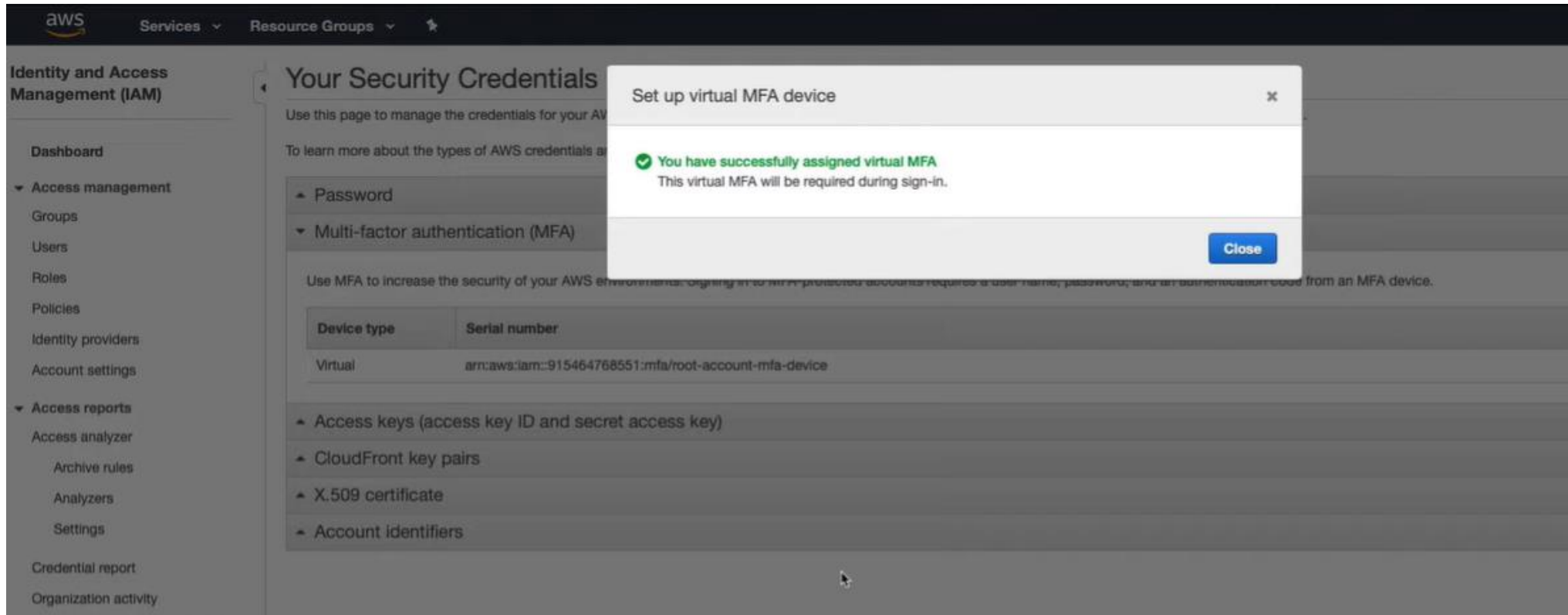
Alternatively, you can type the secret key. [Show secret key](#)

MFA code 1: 640152

MFA code 2: 736525

Buttons: Cancel, Previous, Assign MFA

Securing Root User With MFA



Exercise: Creating A Manager IAM User With Built-in Policies

In this exercise, you will create an IAM user for a manager, and apply built-in IAM policies.

Instructions

Create an IAM user

Name the user "manager"

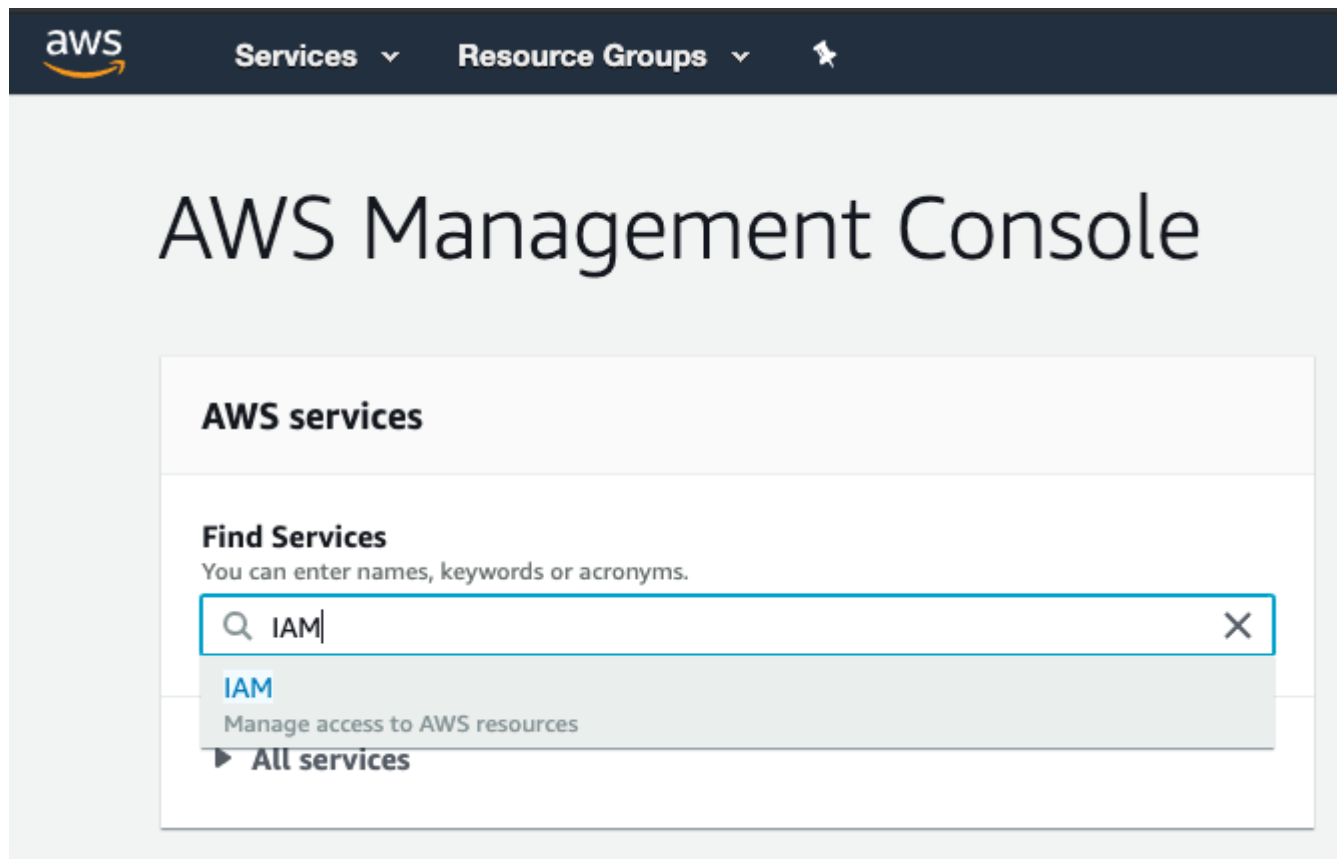
Provide this user with:

- IAM Full Access permissions
- S3 Full Access permissions
- EC2 Full Access permissions

Exercise: Creating A Manager IAM User With Built-in Policies

Creating An IAM User

While logged in as the root account user, navigate to the IAM console.



1. From the left sidebar click on **Users** to get into the Users page
2. Click the **Add User** button and set the **User name** to **manager**
3. Select the **AWS Management Console Access** access type
4. Leave the **Autogenerated password** on
5. Uncheck the option for **Require password reset**
6. Click on the **Next: Permissions** button

The screenshot shows the AWS IAM 'Add user' console. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a star icon. On the right, there are notification and user profile icons. The main heading is 'Add user', with a progress indicator showing three steps: 1 (selected), 2, and 3. The first step, 'Set user details', includes a text input for 'User name*' containing 'manager' and a link to 'Add another user'. The second step, 'Select AWS access type', includes a description of access types and two radio button options for 'Access type*': 'Programmatic access' and 'AWS Management Console access' (which is selected). Below this, there are radio button options for 'Console password*': 'Autogenerated password' (selected) and 'Custom password' (with an empty input field). At the bottom, there is an unchecked checkbox for 'Require password reset' with a description of the policy.

aws Services ▾ Resource Groups ▾ ☆

Add user 1 2 3

Set user details

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

User name*

[+ 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

Require password reset ☐ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

7. Click on the **Attach existing policies directly** button
8. Search for **IAMFullAccess** and select it

Add user

1

2

3

4

5

▼ Set permissions



Add user to group



Copy permissions from
existing user



Attach existing policies
directly

Create policy



Filter policies ▼

Q IAMFullAccess|

Showing 1 result

Policy name ▼

Type

Used as



IAMFullAccess

AWS managed

None

9. Search for **S3FullAccess** and select it

Add user

1 2 3 4 5

▼ Set permissions



Add user to group



Copy permissions from
existing user



Attach existing policies
directly


Create policy



Filter policies ▼

Q S3FullAccess

Showing 1 result


	Policy name ▼	Type	Used as
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	AWS managed	None


10. Search for **EC2FullAccess** and select it


Add user

- 1
- 2
- 3
- 4
- 5

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly


Create policy

↺

Filter policies ▼

Q EC2FullAccess

Showing 1 result

	Policy name ▼	Type	Used as
<input checked="" type="checkbox"/>	 AmazonEC2FullAccess	AWS managed	None

11. Click on the **Next: Tags** button. We don't need to add any tags at the moment, so skip the tags by clicking on the **Next: Review** button

Add user



Review

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

User details

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

Permissions summary

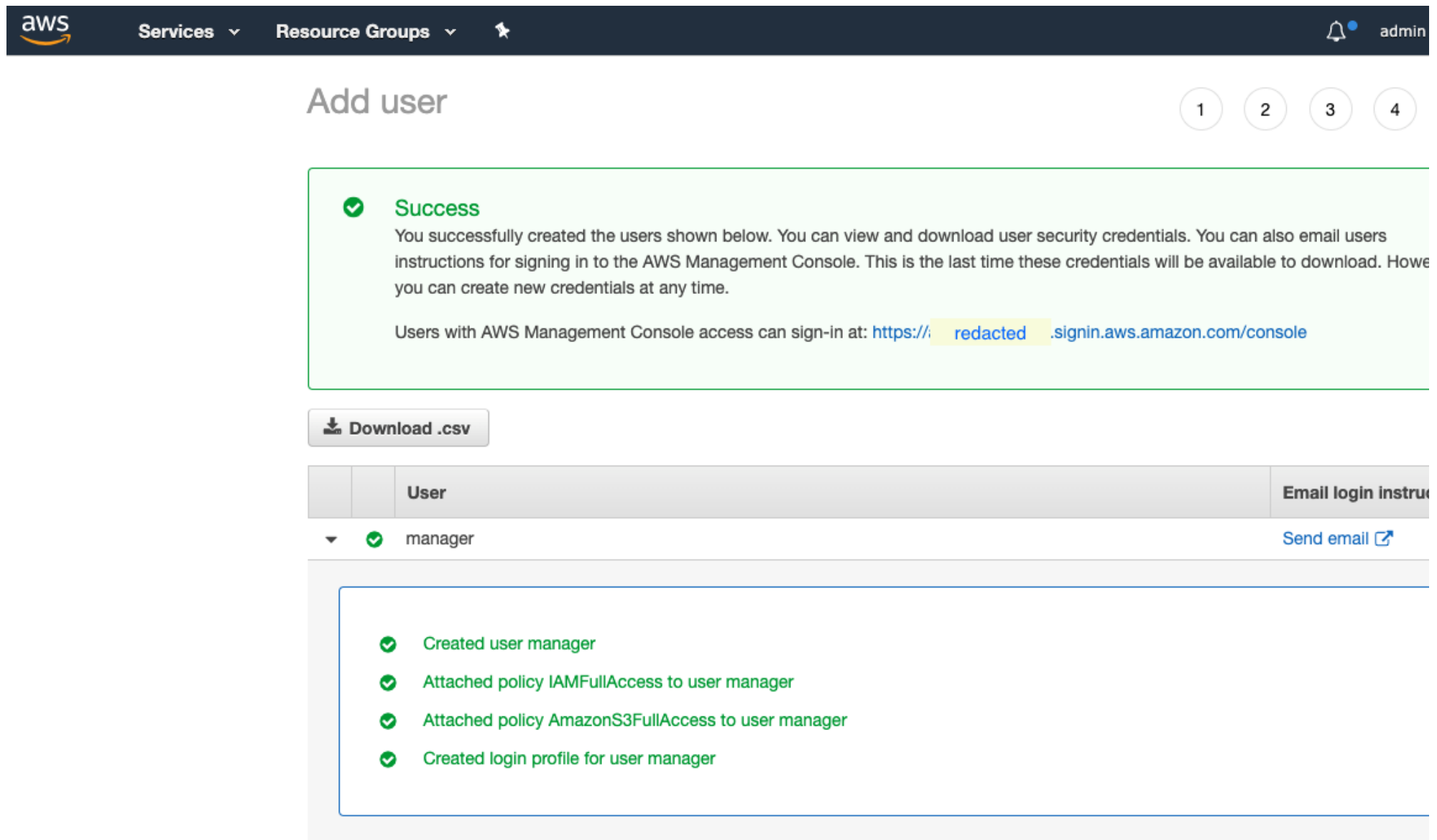
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess
Managed policy	AmazonEC2FullAccess
Managed policy	IAMFullAccess

Tags

No tags were added.

12. Click on the **Create user** button to create the user



The screenshot shows the AWS IAM console 'Add user' page. At the top, the AWS logo and navigation menu are visible. The page title is 'Add user'. On the right, there are four numbered steps: 1, 2, 3, and 4. A green success message box indicates that the user was created successfully. Below the message is a 'Download .csv' button. A table lists the created user, 'manager', with a 'Send email' link. A detailed list of actions performed for the user is shown in a box below the table.

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
<div>▼ manager</div>	Send email

- Created user manager
- Attached policy IAMFullAccess to user manager
- Attached policy AmazonS3FullAccess to user manager
- Created login profile for user manager

13. Copy and save both the password (show password) and the login URL somewhere you will be able to access it later

Exercise: Securing IAM User With MFA

Instructions


- If you have not yet done so, you must first create a **manager** AWS account
- Install an MFA app on your phone - the **Google Authenticator** app ([Android](#), [iOS](#)) is a good choice
- Secure the manager account with MFA
- Log out and log back in to verify that MFA is enabled

Navigate to the IAM console and select the user you want to secure with MFA (in this series of exercises this would be the **manager** user).

1. Click on the user account and open the **Security Credentials** tab

[Users](#) > manager

Summary

User ARN arn:aws:iam:: redacted :user/manager 

Path /

Creation time 2020-04-06 14:18 PDT

Permissions

Groups

Tags

Security credentials

Access Advisor

Sign-in credentials

Summary

- Console sign-in link: <https:// redacted l.signin.aws.amazon.com/console>

Console password Enabled (never signed in) | [Manage](#)

Assigned MFA device Not assigned | [Manage](#)

Signing certificates None 

2. Click **Manage** next to the **Assign MFA device**
3. Leave the default **Virtual MFA device** option on and click continue
4. Click the **Show QR code** in the empty square

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

5. Open the **Google Authenticator** app on your phone and click the **Scan a barcode** camera icon
6. Scan the barcode
7. Type the code you see on your phone into the **MFA code 1** field
8. Wait for the Google Authenticator app to generate the next code
9. Type the next consecutive code into the **MFA code 2** field and click the **Assign MFA** button
10. Using a new incognito or private browser window to login with this user and the MFA code from your phone

If you have configured MFA correctly you should be able to log in.

If not:

1. Log in as the root user
2. Proceed to the IAM service console
3. Click on **Users**
4. Select the **manager** user
5. Visit the **Security credentials** tab
6. Next to **Assigned MFA device**, click **Manage**
7. Remove the assigned MFA device
8. Log out of the root user account
9. Log back in with the manager account
10. Try again to configure MFA

Exercise: Creating S3 Bucket And Uploading Content

Instructions

If you have not done so already, register with AWS and authenticate as the **manager** user

Create a bucket in the **us-west-2 Oregon** region

Create 2 folders in the bucket: "exercise" and "manager"

Upload content to both folders (a single file in each folder will suffice)

Note: Please do not delete the bucket until the end of this course. Deleting a bucket takes a long time. If you delete the bucket and then try to create it again later, you may run into errors.

STORAGE

Free Tier

12 MONTHS FREE

Amazon S3

5 GB

of standard storage

Secure, durable, and scalable object storage infrastructure.

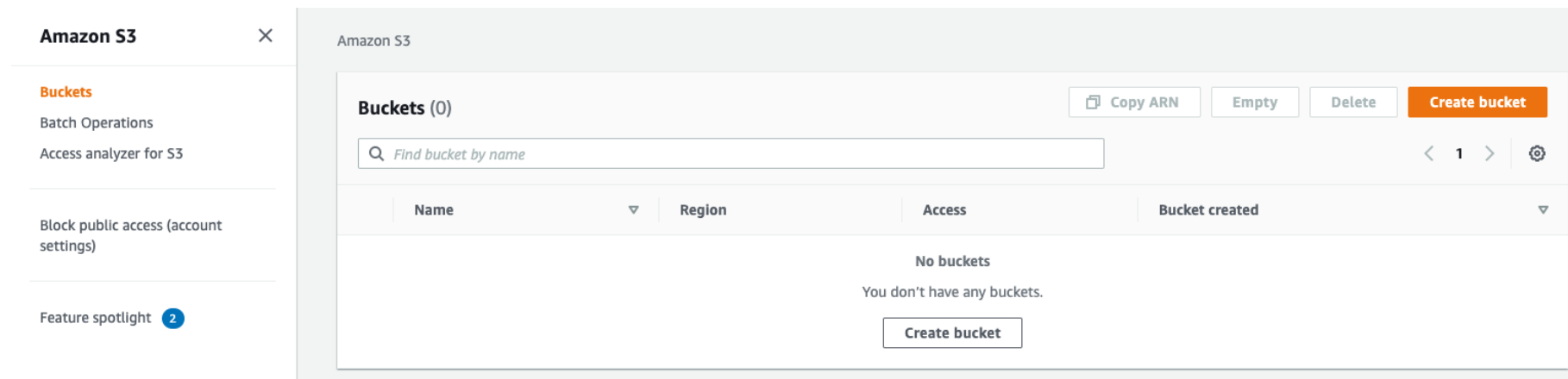
5 GB of Standard Storage

20,000 Get Requests

2,000 Put Requests

Part-1: Creating The Bucket

1. Log out of the root account user by clicking on the top right email next between the **Bell icon** and the **Global** dropdown menu
2. Log in to the console as the manager, using the information from you've got from the previous step
3. Navigate to the S3 console
4. Create a new bucket (remember that bucket names are globally unique across all AWS accounts)



Note that if a bucket name already exists you will get a warning.

Note:

Deleting a bucket takes time, so creating the same bucket name after a deletion would not allow you to create the bucket and will result in a "Bucket already exists error"



Create bucket

General configuration

Bucket name

ami-test


 Bucket with the same name already exists

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#) 

Region

US West (Oregon) us-west-2

Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

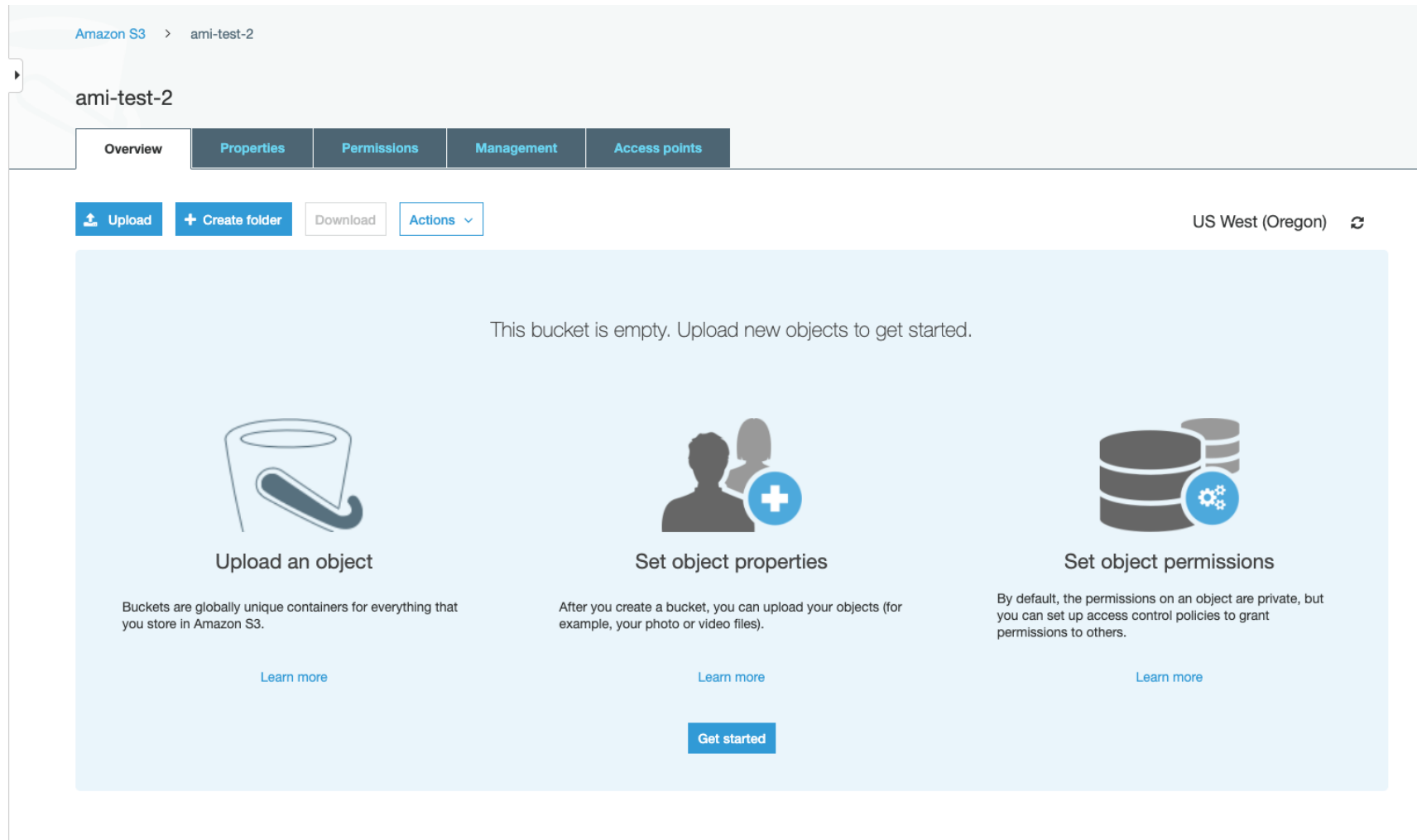
- ☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☒ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☒ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

► Advanced settings

Cancel

Create bucket

5. Once the bucket is created, click on the **Create folder** button to create a **manager** folder



ami-test-2

Overview

Properties

Permissions

Management

Access points

🔍 Type a prefix and press Enter to search. Press ESC to clear.

📁 Upload

+ Create folder

Download

Actions ▾

☐ Name ▾

Last r



When you create a folder, S3 console creates an object with the above name appended by suffix "/" and that object is displayed as a folder in the S3 console. Choose the encryption setting for the object:

☒ None (Use bucket settings)

☐ AES-256

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

☐ AWS-KMS

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Save

Cancel



6. Create another folder called exercise



Amazon S3 > ami-test-2

ami-test-2

Overview Properties Permissions Management Access points

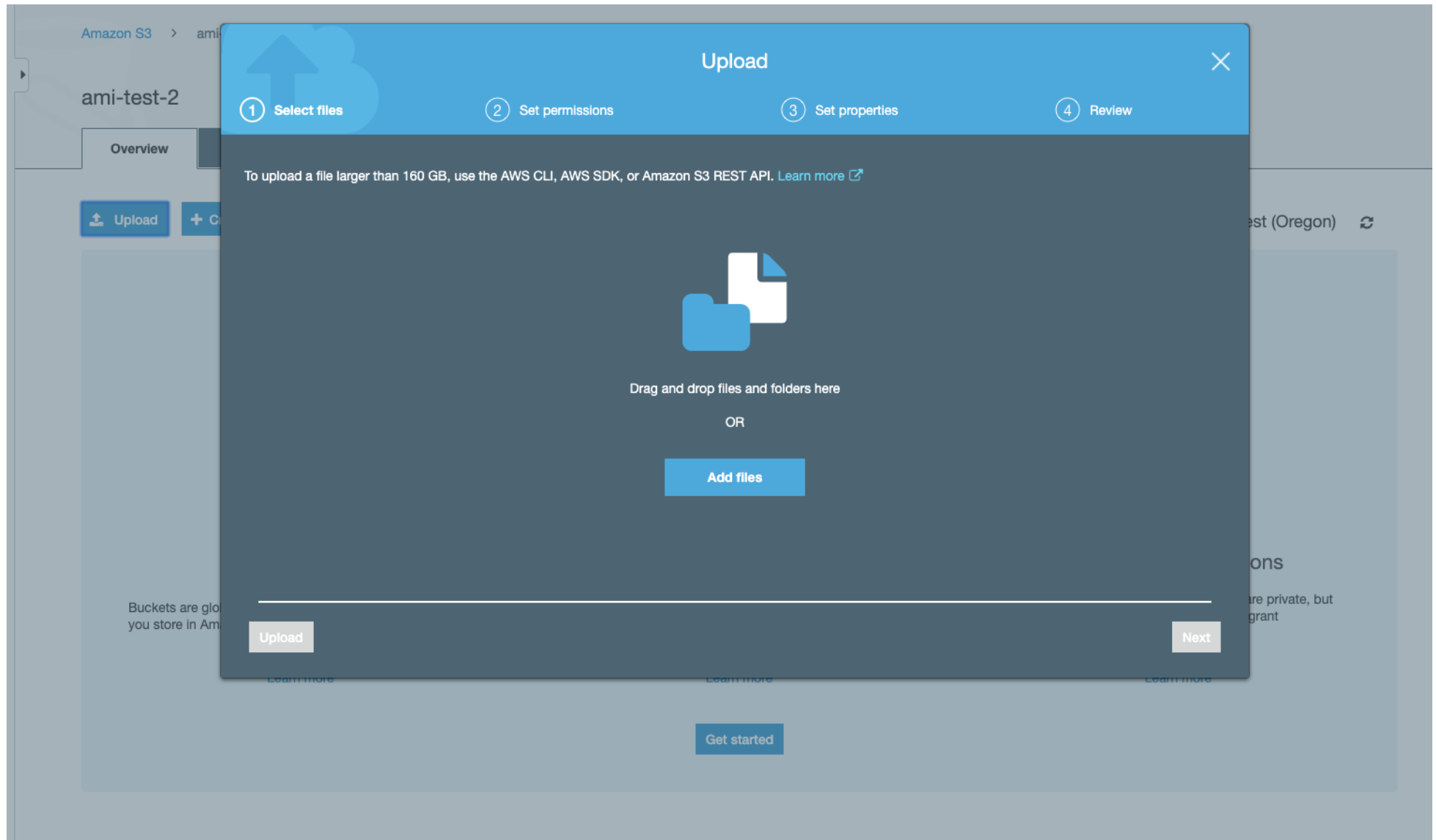
🔍 Type a prefix and press Enter to search. Press ESC to clear.

 Upload  Create folder Download Actions ▾

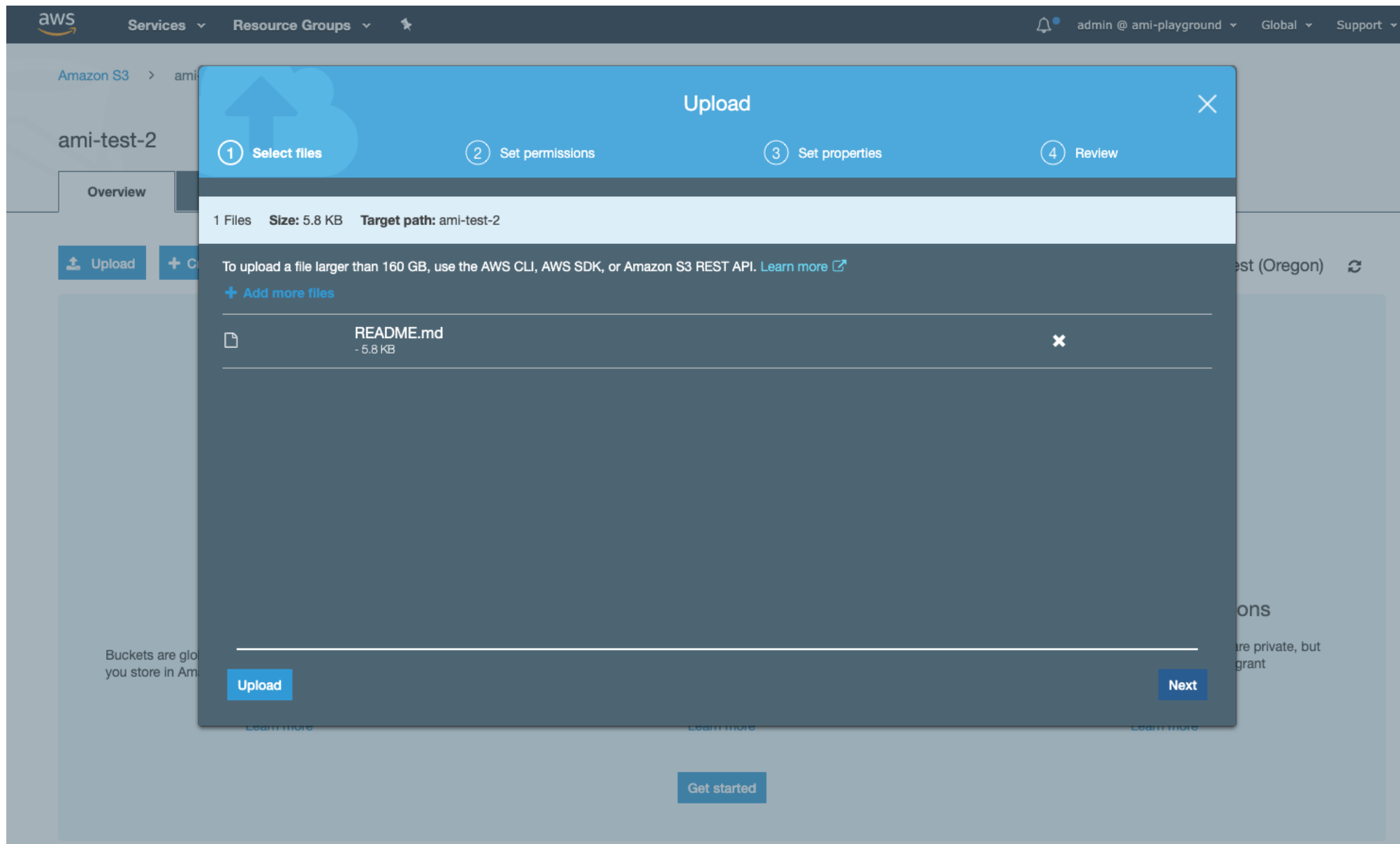
<input type="checkbox"/>	Name ▾	Last r
<input type="checkbox"/>	 exercise	--
<input type="checkbox"/>	 manager	--

7. Click on the **exercise** folder to get into that folder

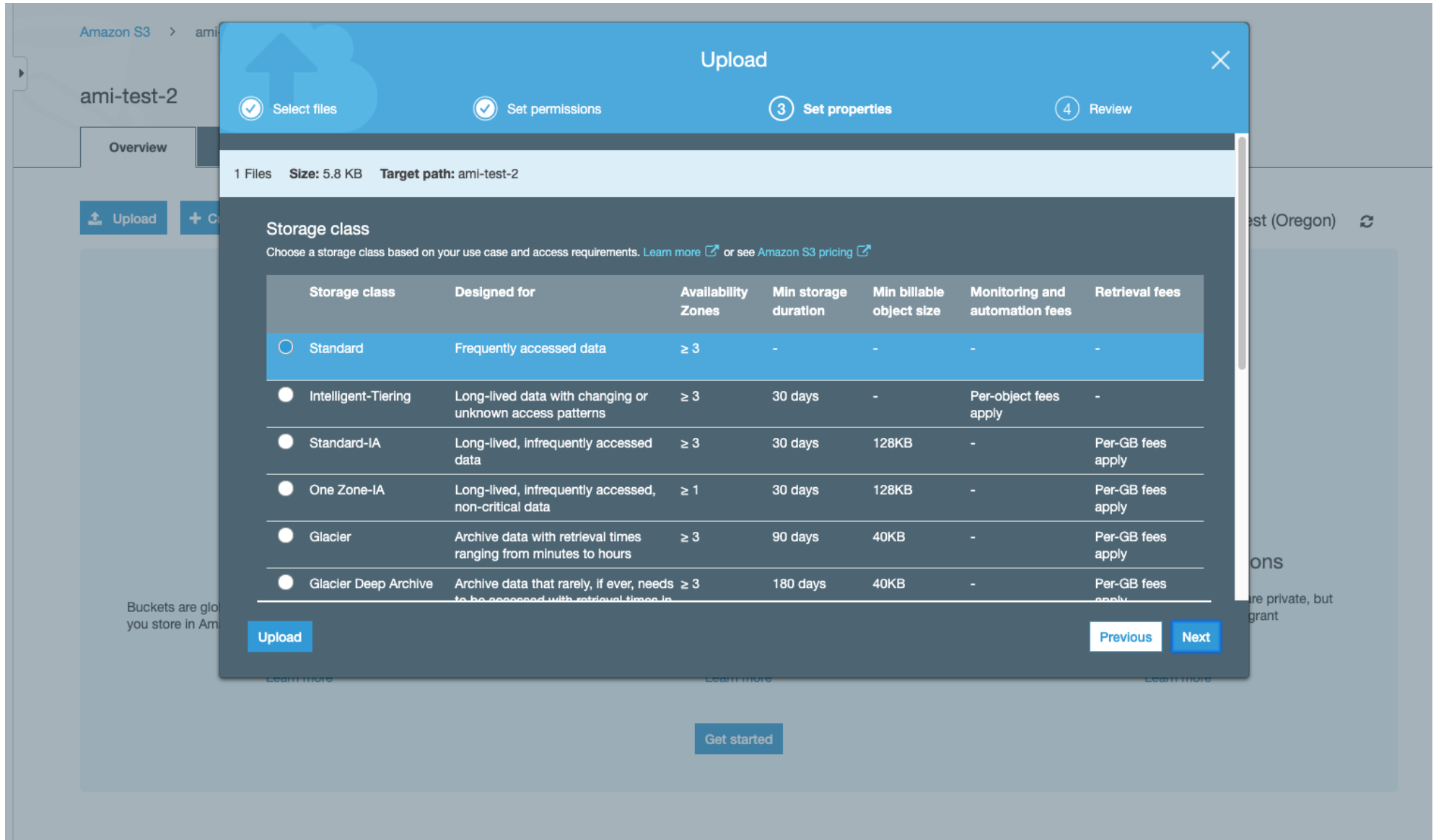
8. Click on the **Upload** button to upload a file (any file) into that folder



9. Either drag and drop a file onto the window or click the **Add files** button to start the upload process



10. Click the **Next** button to see the list of default permissions for this file (we will use IAM permission to access it rather than resource permissions)
11. Click Next to see the S3 storage classes, and leave the default **Standard** class selected



The screenshot shows the Amazon S3 Upload wizard for a bucket named 'ami-test-2'. The wizard is in the 'Set properties' step (step 3 of 4). The 'Storage class' section is active, displaying a table of storage options. The 'Standard' class is selected by default.

Upload

1 Files Size: 5.8 KB Target path: ami-test-2

Storage class
Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed with retrieval times in	≥ 3	180 days	40KB	-	Per-GB fees apply

Upload **Previous** **Next**

[Get started](#)

12. Click the **Upload** button to start the upload.

The screenshot shows the AWS IAM console interface. In the background, the 'Overview' tab for the IAM user 'ami-test-2' is visible, featuring an 'Upload' button. A modal window titled 'Upload' is open in the foreground, displaying a four-step progress bar: 'Select files' (checked), 'Set permissions' (checked), 'Set properties' (checked), and 'Review' (active, indicated by a circled '4'). The modal is divided into three sections: 'Files', 'Permissions', and 'Properties'. The 'Files' section shows '1 Files' and 'Size: 5.8 KB' with an 'Edit' link. The 'Permissions' section shows '1 grantees' with an 'Edit' link. The 'Properties' section includes 'Encryption' (No), 'Storage class' (Standard), 'Metadata', and 'Tag', each with an 'Edit' link. At the bottom right of the modal are 'Previous' and 'Upload' buttons. The background interface also shows a 'Get started' button at the bottom center.

ami-test-2

- Overview
- Properties
- Permissions
- Management
- Access points


Q

Type a prefix and press Enter to search. Press ESC to clear.

- Upload
- Create folder
- Download
- Actions

US West (Oregon)

Viewing 1 to 1

<input type="checkbox"/>	Name	Last modified	Size	Storage class
<input type="checkbox"/>	 README.md	Apr 6, 2020 11:15:54 AM GMT-0700	5.8 KB	Standard

Viewing 1 to 1

Monitoring your AWS costs

All AWS services are a pay-as-you-go service, so we urge our students to closely monitor their usage costs and if they have adequate credits available to complete their project/task. Follow the instructions below to do that:

Step 1. Log into your [AWS account](#).

Step 2. Examine your costs

Go to <https://console.aws.amazon.com/billing/>

You should see the following billing dashboard where it will show your costs.

Monitoring your AWS costs

Home

Cost Management

Cost Explorer

Budgets

Budgets Reports

Savings Plans

Cost & Usage Reports

Cost Categories

Cost allocation tags

Billing

Bills

Orders and invoices

Credits

Preferences

Billing preferences

Payment methods

Consolidated billing

Tax settings

Billing & Cost Management Dashboard



Getting Started with AWS Billing & Cost Management

- Manage your costs and usage using [AWS Budgets](#)
- Visualize your cost drivers and usage trends via [Cost Explorer](#)
- Dive deeper into your costs using the [Cost and Usage Reports](#) with [Athena integration](#)
- **Learn more:** Check out the [AWS What's New webpage](#)

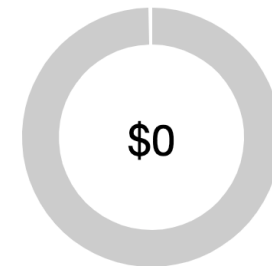
Do you have Reserved Instances (RIs)?

- Access the RI Utilization & Coverage reports—and RI purchase recommendations—via [Cost Explorer](#).

Month-to-Date Spend by Service

Bill Details

The chart below shows the proportion of costs spent for each service you use.



Spend Summary

Cost Explorer

Welcome to the AWS Billing & Cost Management console. Your last month, month-to-date, and month-end forecasted costs appear below.

Current month-to-date balance for May 2020

\$0.00

\$4 _____

\$3 _____

\$2 _____

No Amount Due

\$0.00

Monitoring your AWS costs

Step 3 (optional). Check the value of your credits.

Click on the "Credits" from the left side menu and the following screen will show with your available credits.

Cost & Usage Reports

Cost Categories

Cost allocation tags

Billing

Bills

Orders and invoices

Credits

Preferences


Billing preferences

Payment methods

Consolidated billing

Tax settings

Security Check ⓘ



Refresh Image

Please type the characters as shown above

By clicking "Redeem" you indicate that you have read and agree to the terms of the AWS Promotional Credit Terms & Conditions located [here](#).

Redeem

The table below displays all AWS credits redeemed by your account. Credits are automatically applied to charges associated with qualifying AWS service usage. Please note that the values for used and remaining credit amounts are updated each month when your invoice is finalized.

Expiration Date	Credit Name	Amount Used	Amount Remaining	Applicable Products
12/31/2020	EDU_ENG_FY2019_IC_Q4_12_UDACITY_75USD	\$0.00	\$75.00	See complete list

Total Credit Amount Remaining (as of 05/01/2020): \$75.00

AWS Elastic Compute Cloud (EC2)

- Resizeable, scalable compute capacity
- Instance sizes are predefined by instance types
- Configuring an instance can be done within the EC2 Launch Wizard:
 - Security groups (i.e. firewall rules)
 - Networking (public or private)
 - Storage size and type
 - Custom provisioning scripts

COMPUTE

Free Tier

12 MONTHS FREE

Amazon EC2

750 Hours

per month

Resizable compute capacity in the Cloud.

750 hours per month of Linux, RHEL, or SLES t2.micro or t3.micro instance dependent on region

750 hours per month of Windows t2.micro or t3.micro instance dependent on region