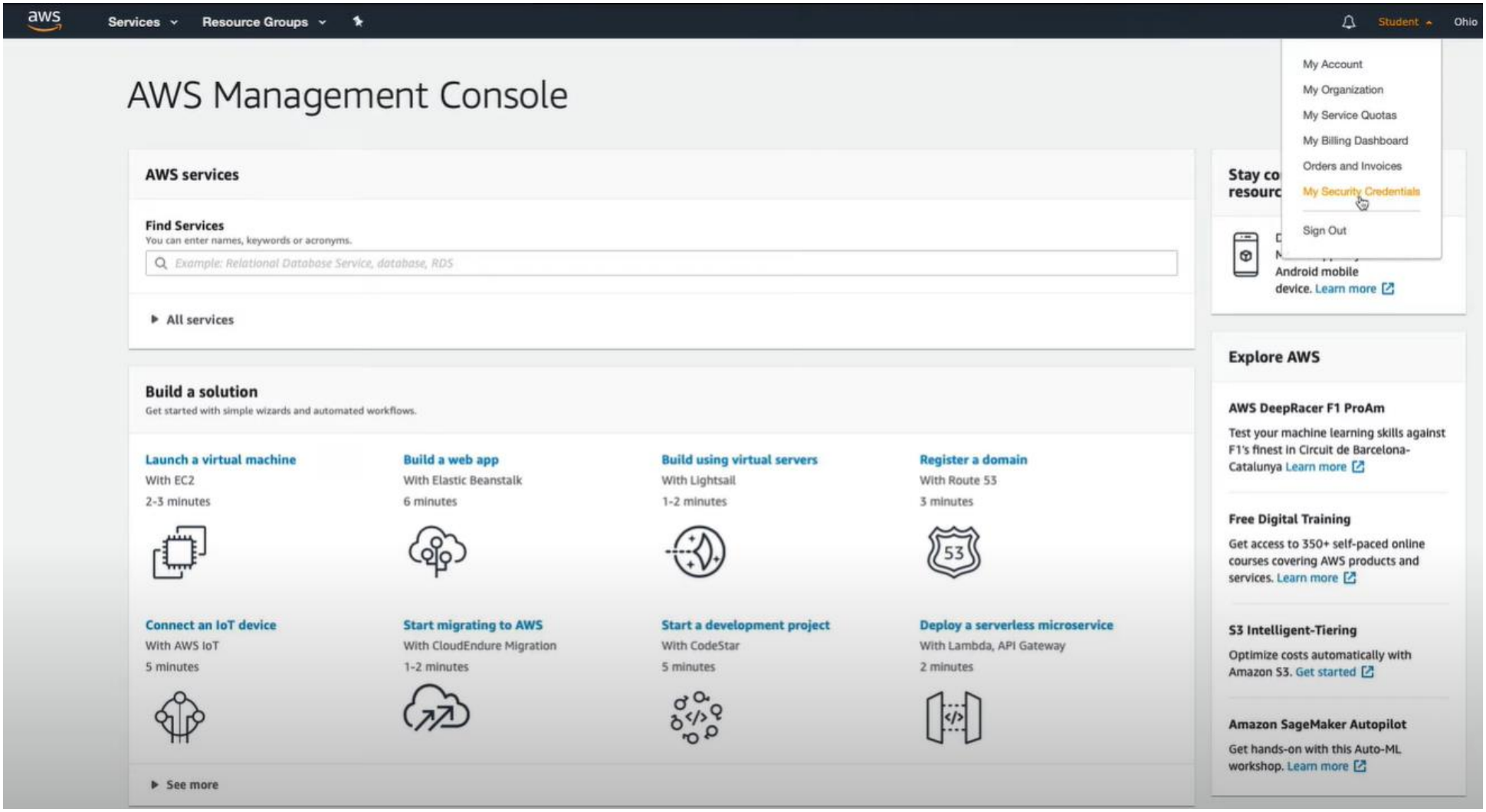
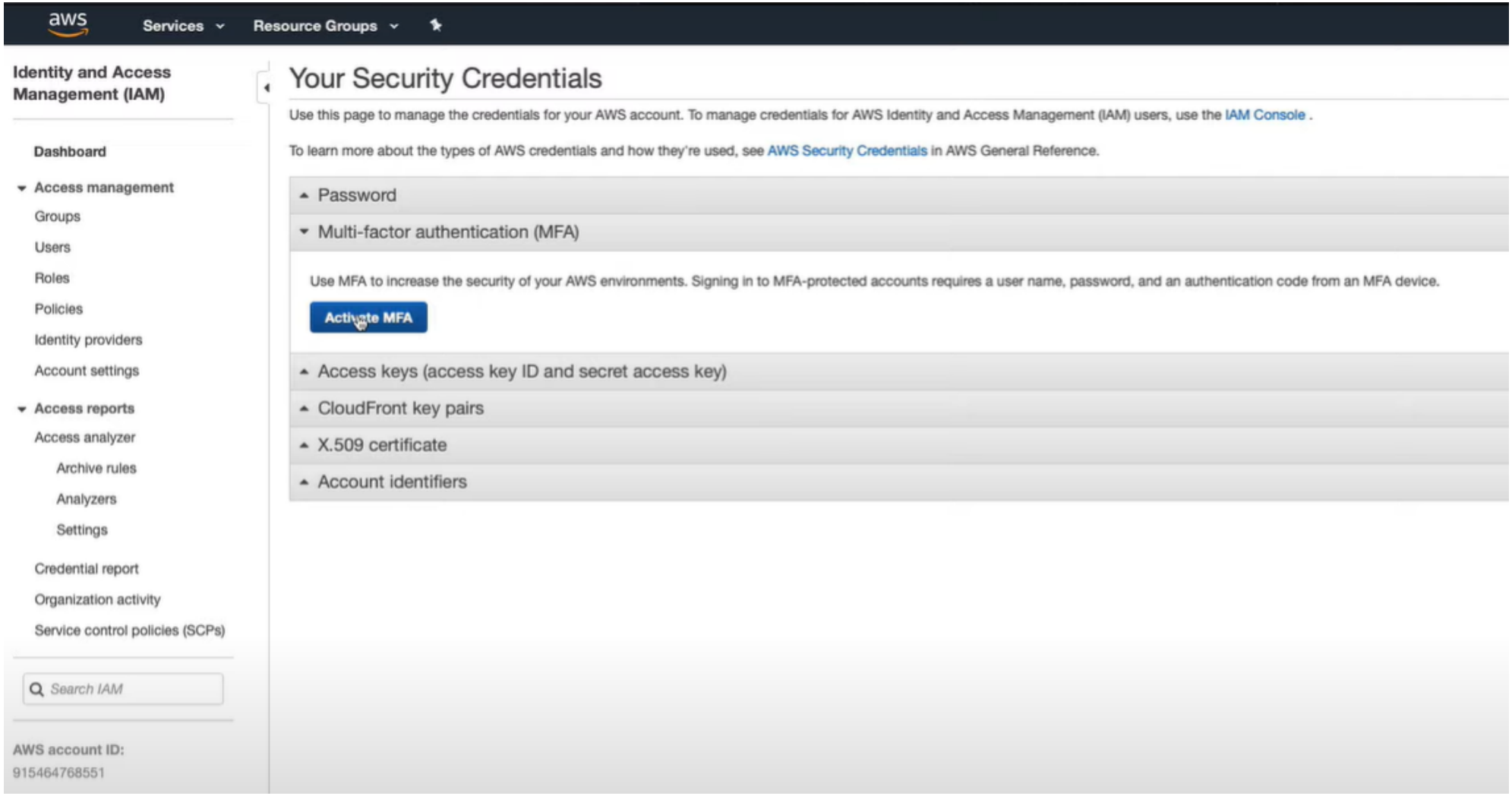
Securing Root User With MFA



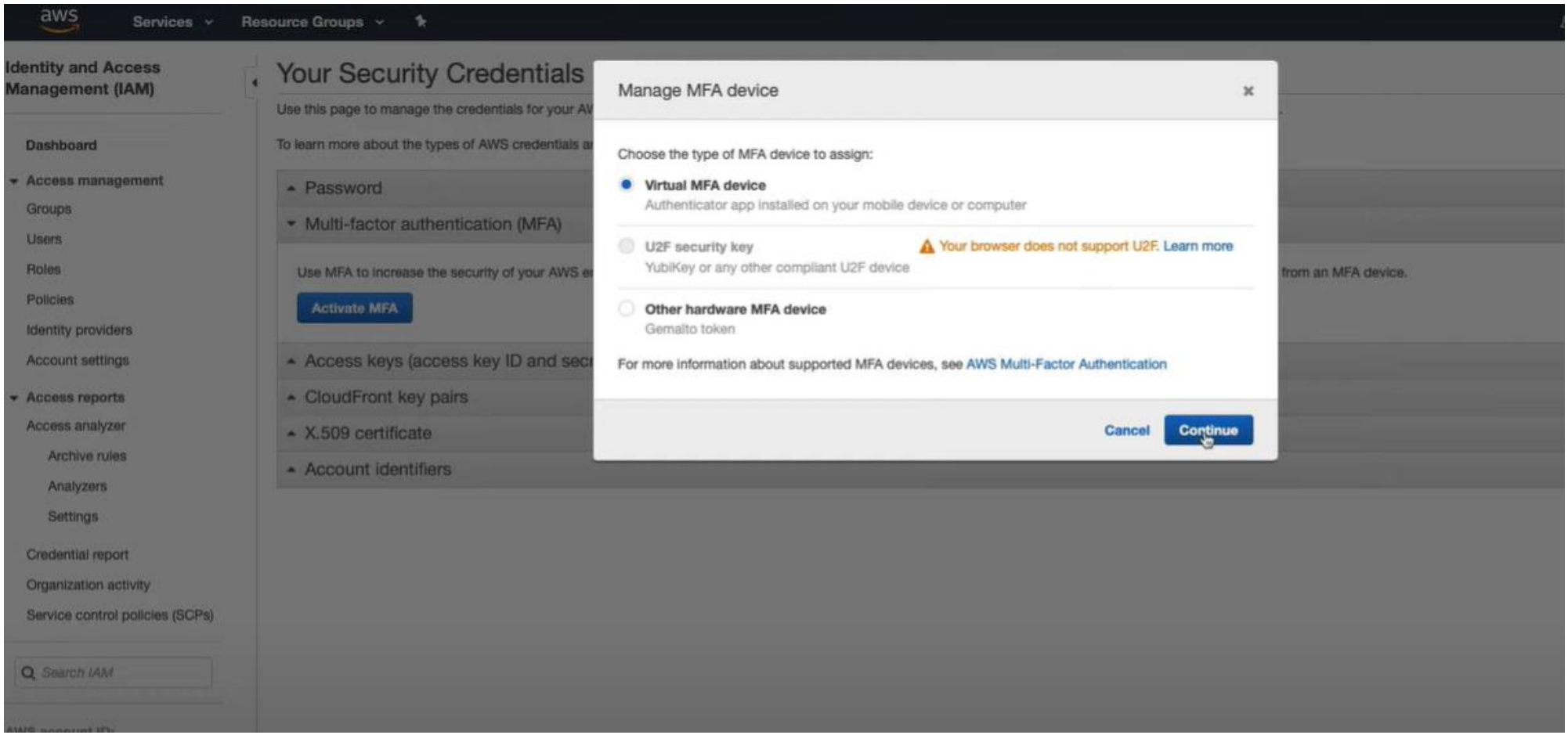
Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

Securing Root User With MFA



Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

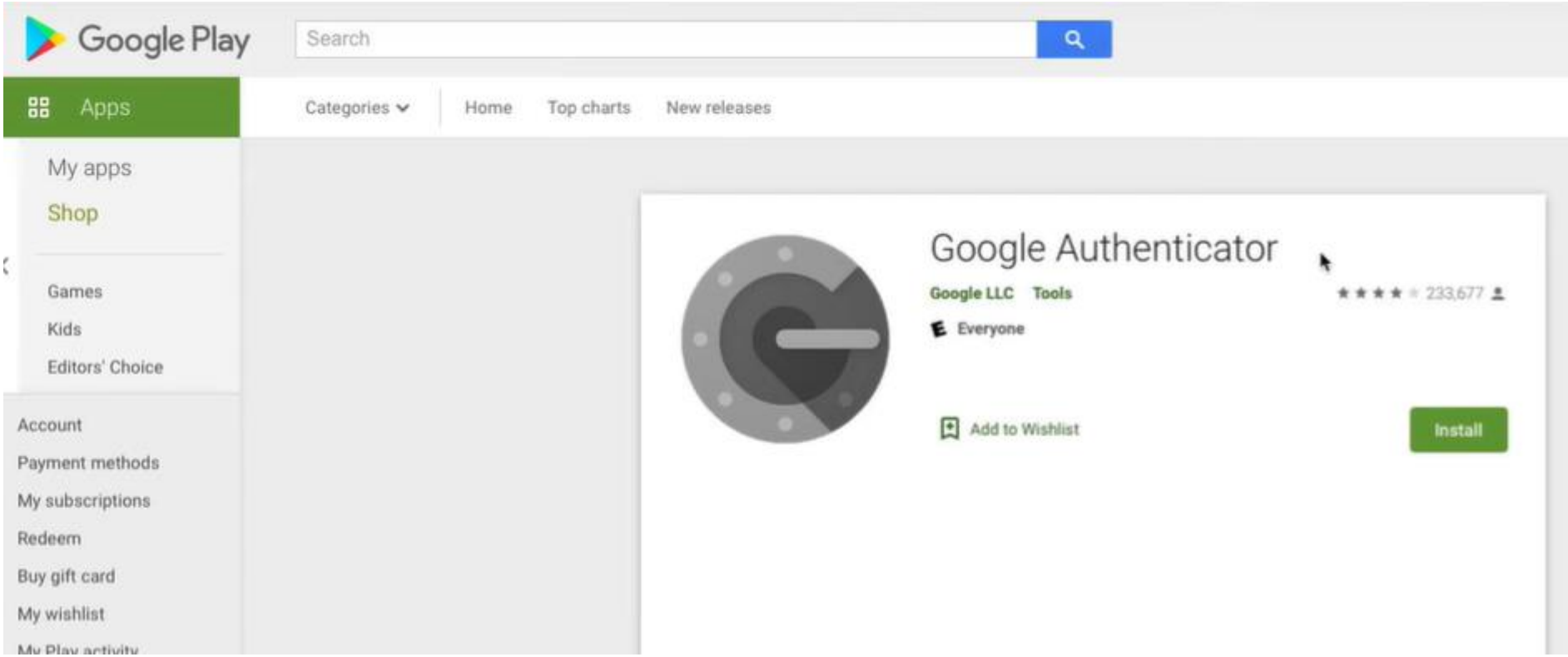
Securing Root User With MFA



Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

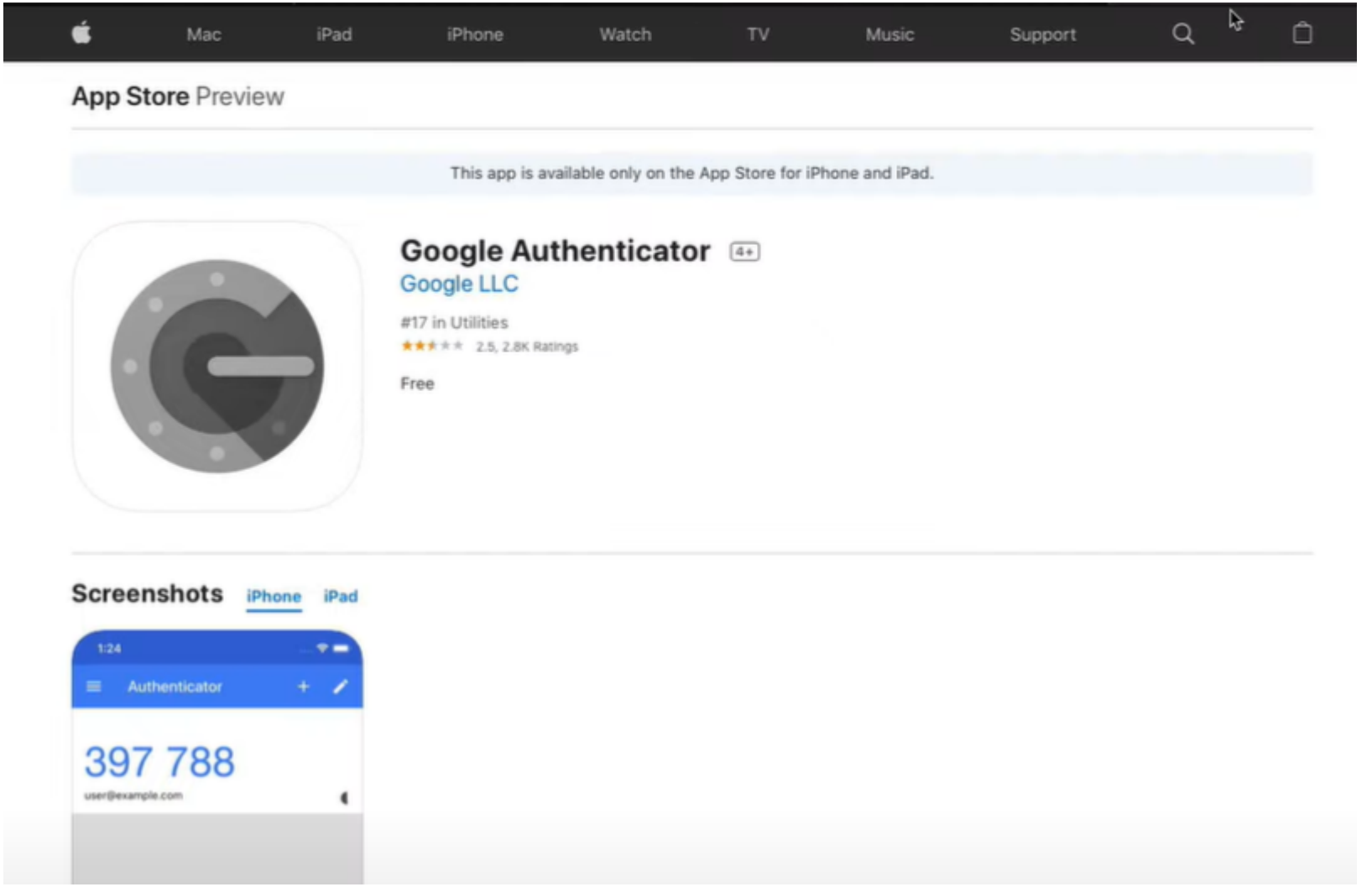
Securing Root User With MFA

Install Google Authenticator app.



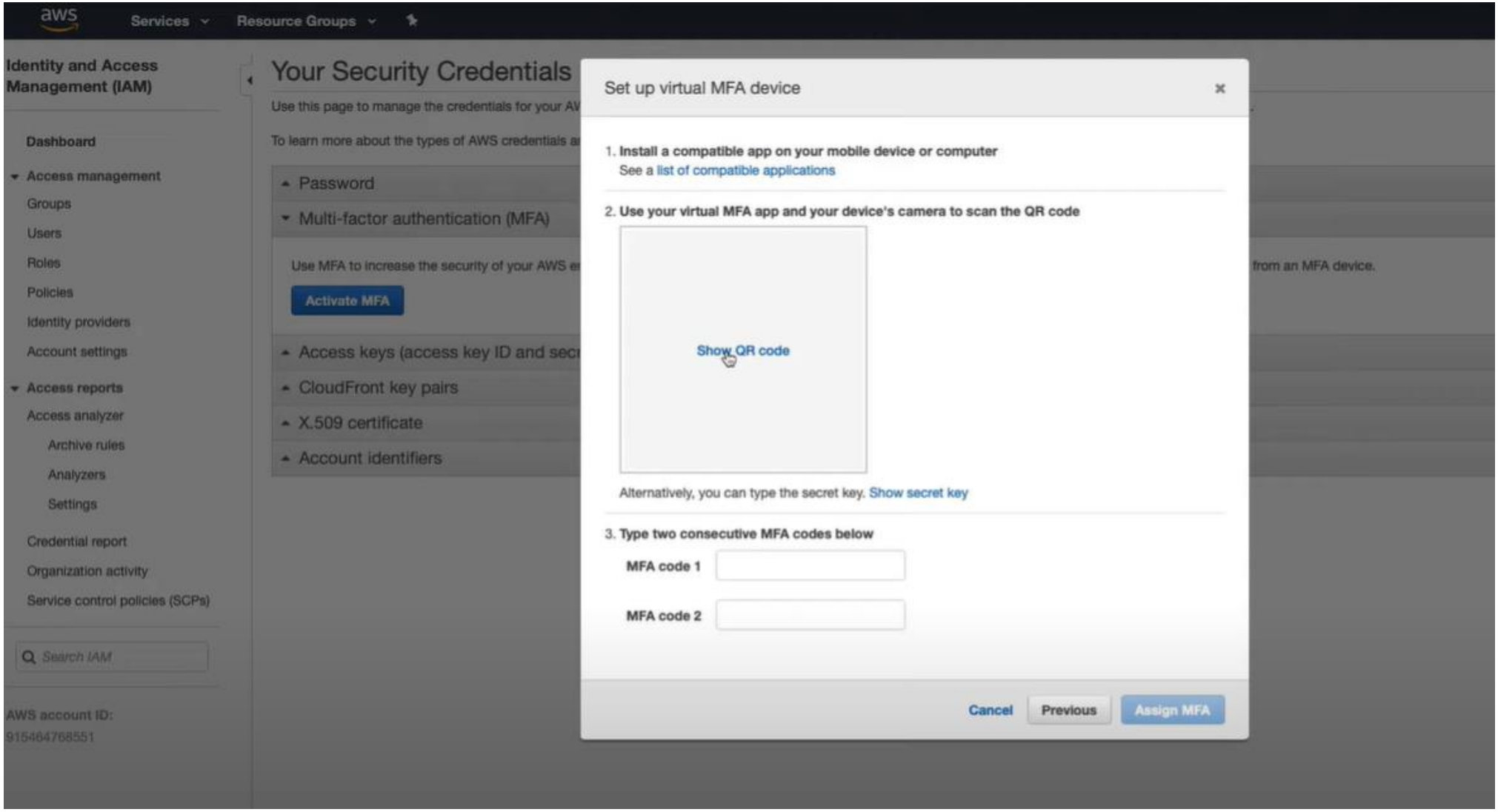
Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

Securing Root User With MFA



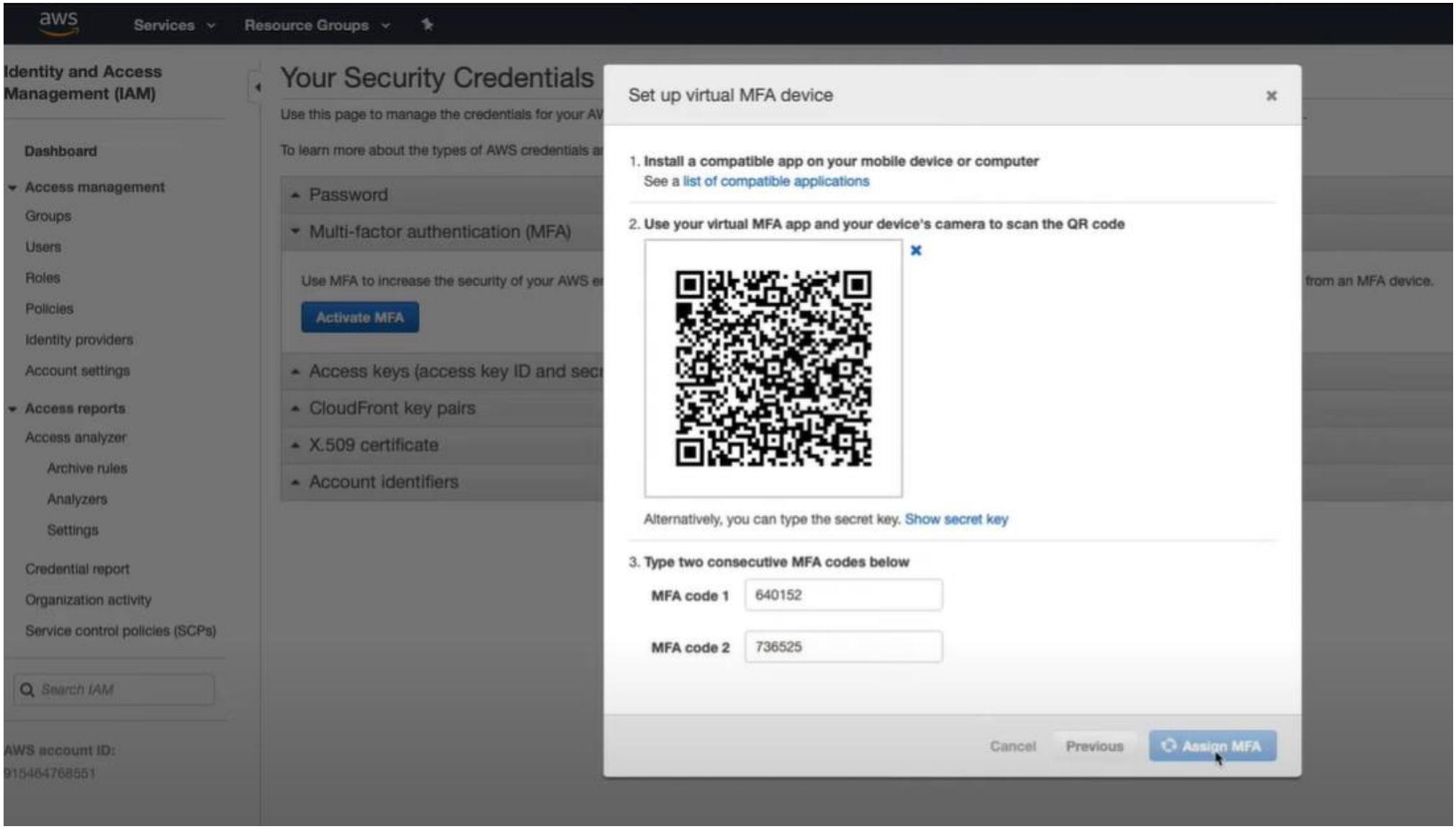
Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

Securing Root User With MFA



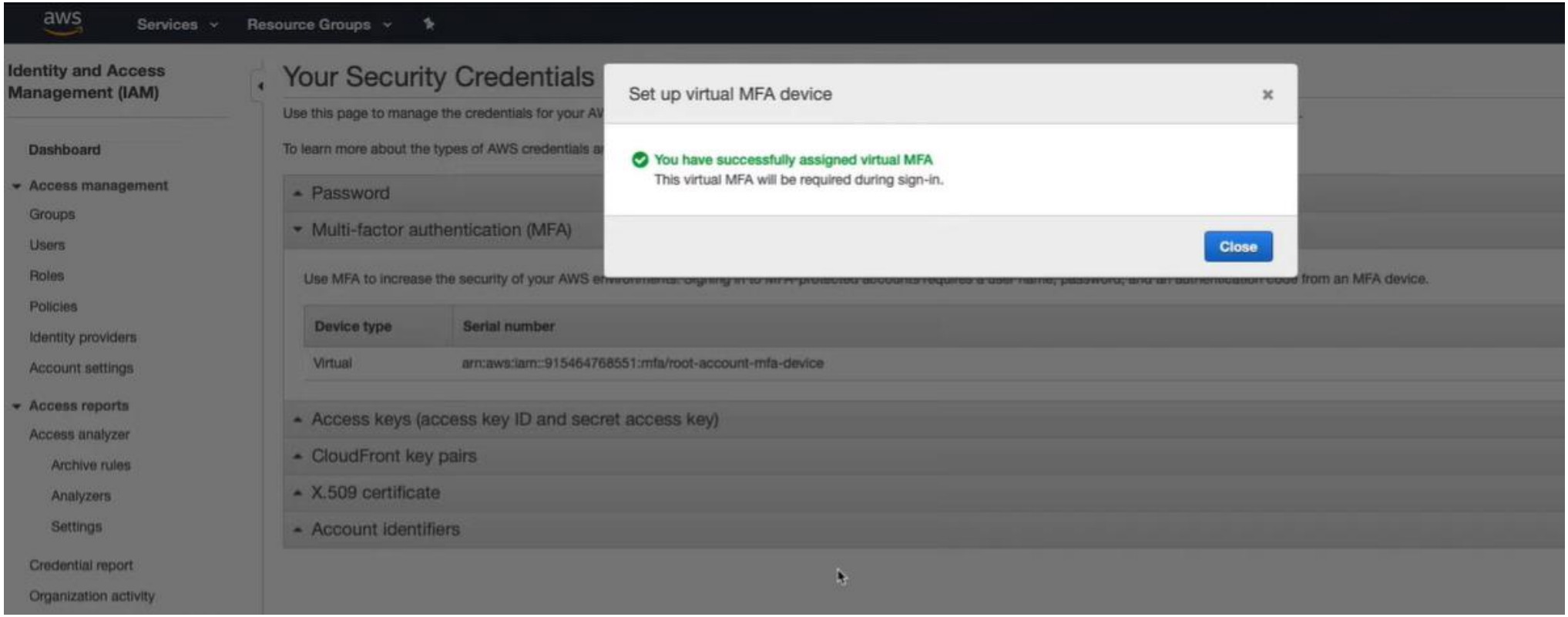
Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

Securing Root User With MFA



Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

Securing Root User With MFA



Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

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"

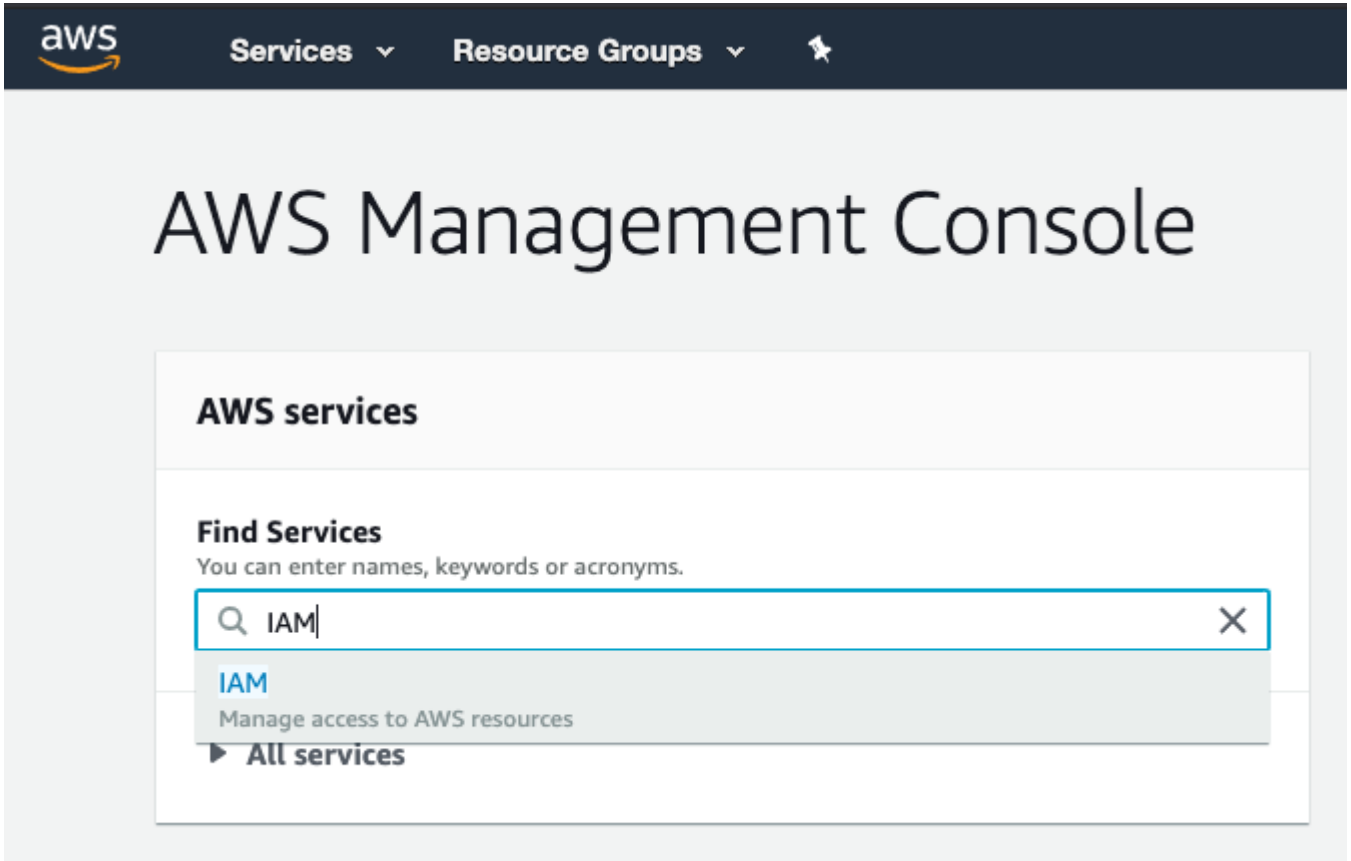
Provide this user with:

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

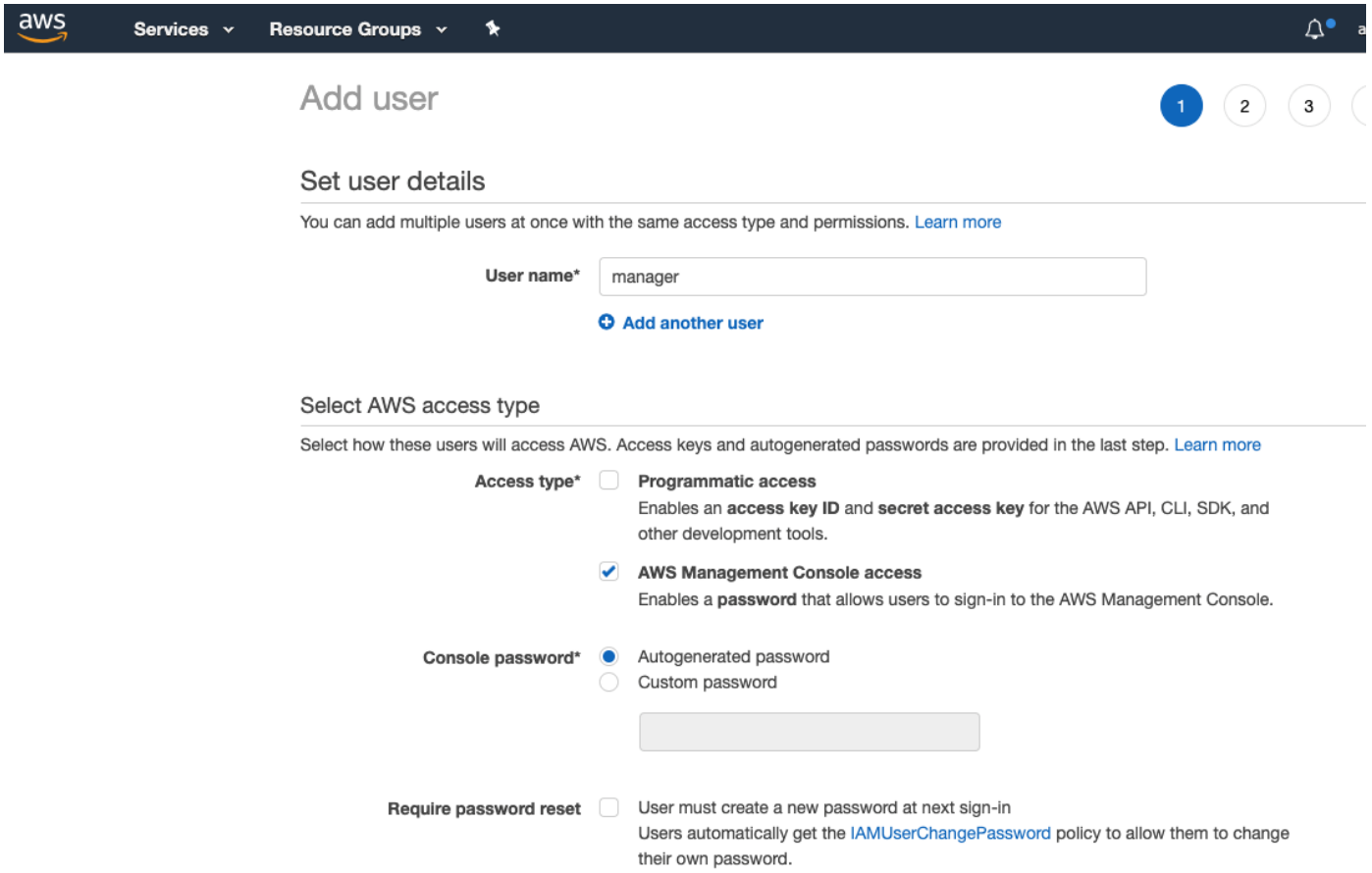
Exercise: Creating A Manager IAM User With Built-in Policies

Creating An IAM User

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

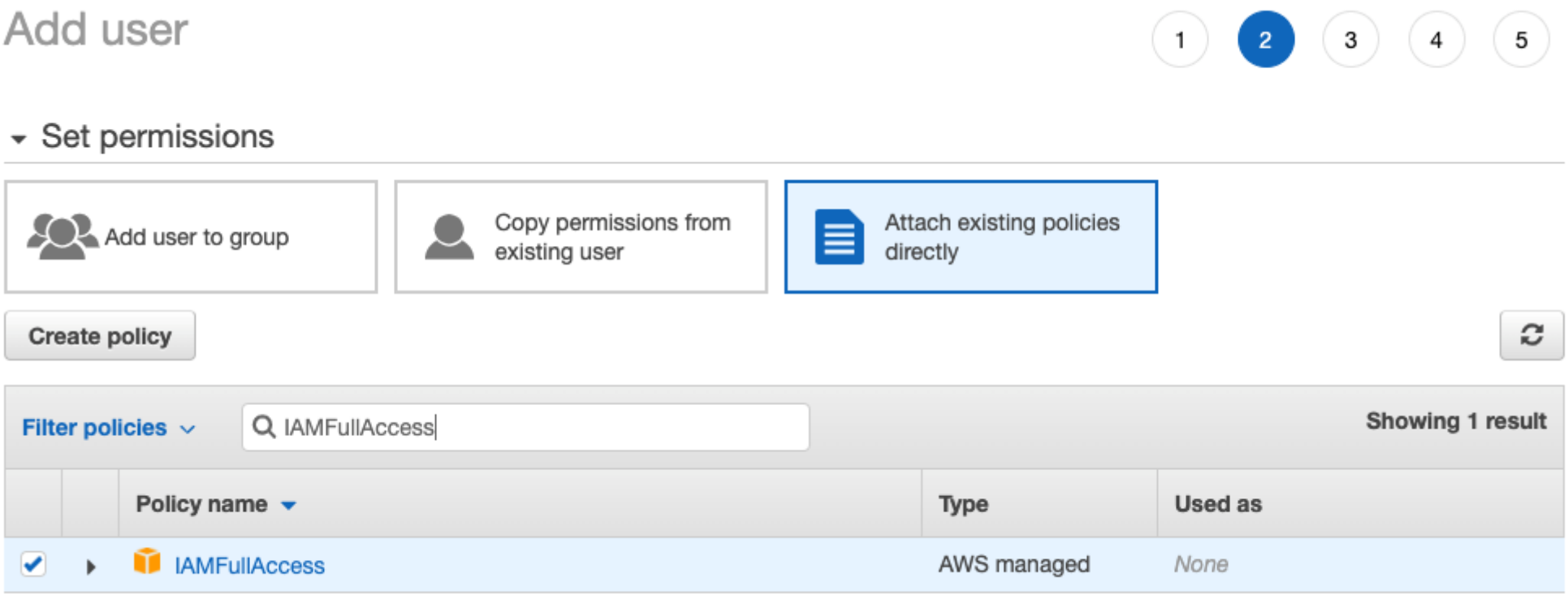


1. From the left sidebar click on **Users** to get into the Users page
2. Click the **Add User** button and set the **User name** to **manager**
3. Select the **AWS Management Console Access** access type
4. Leave the **Autogenerated password** on
5. Uncheck the option for **Require password reset**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

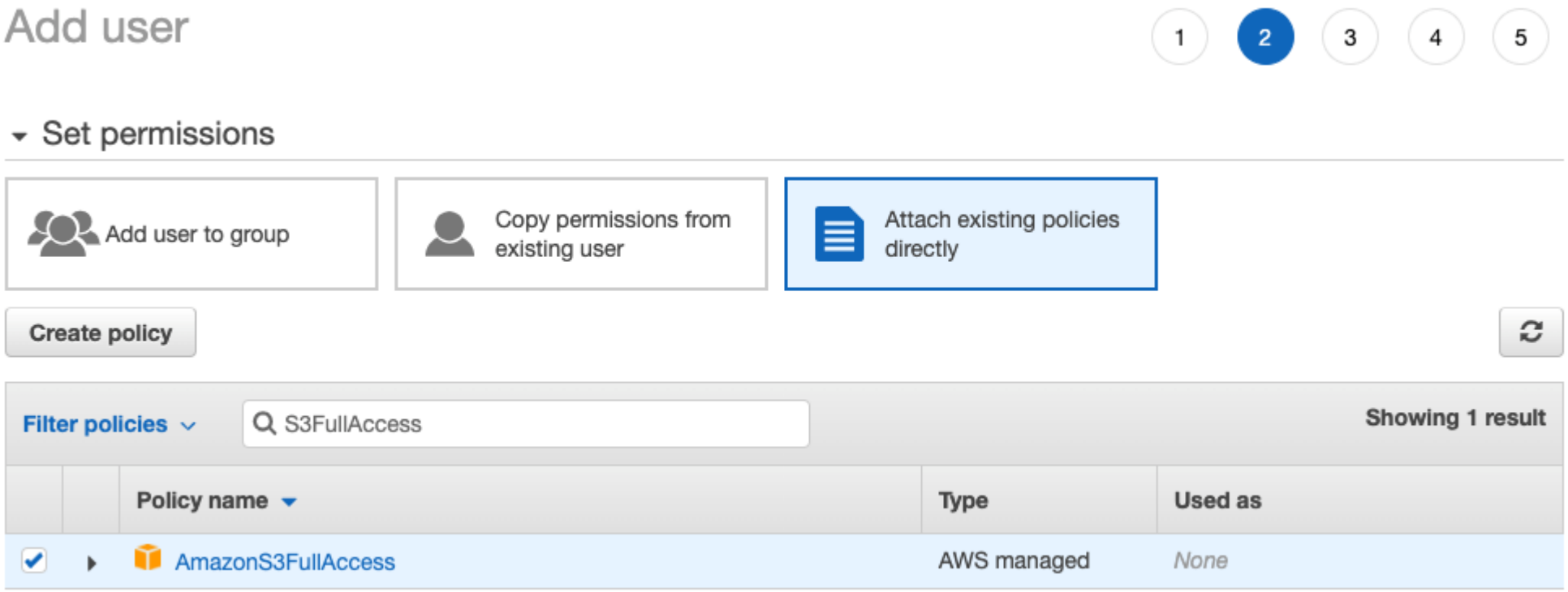


7. Click on the **Attach existing policies directly** button

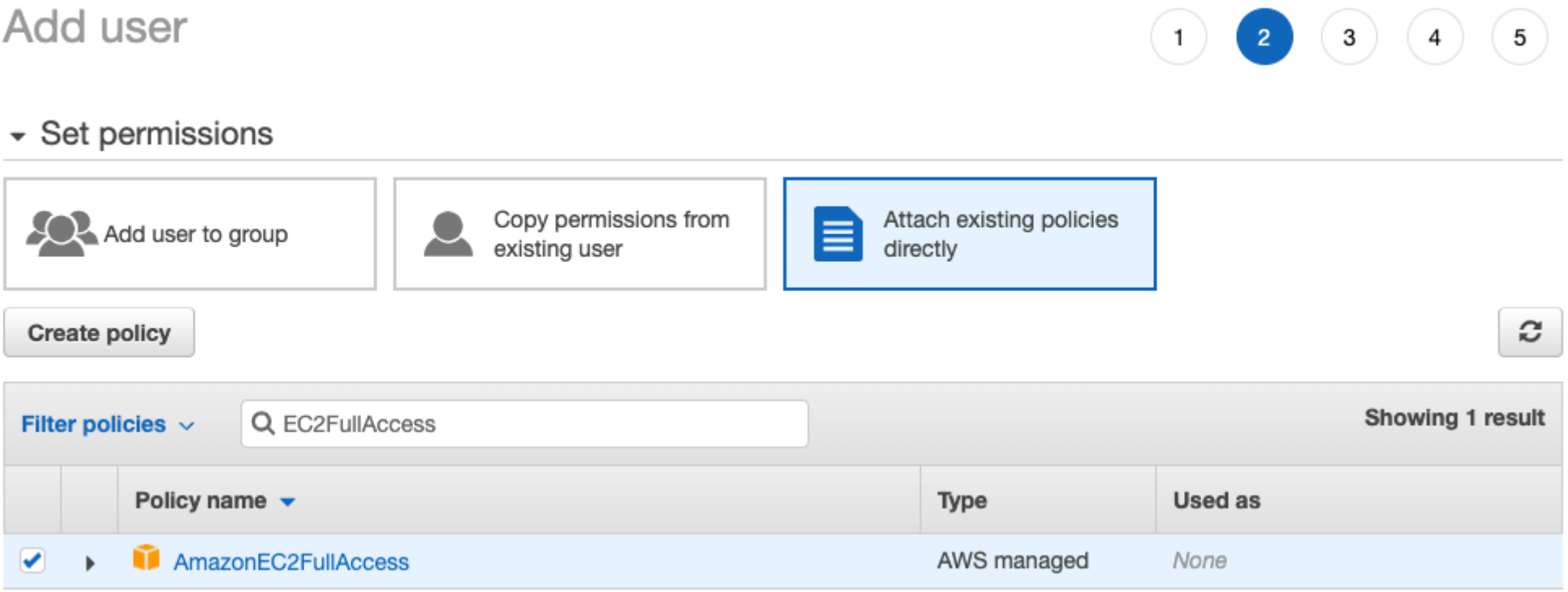
8. Search for **IAMFullAccess** and select it



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



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



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

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	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

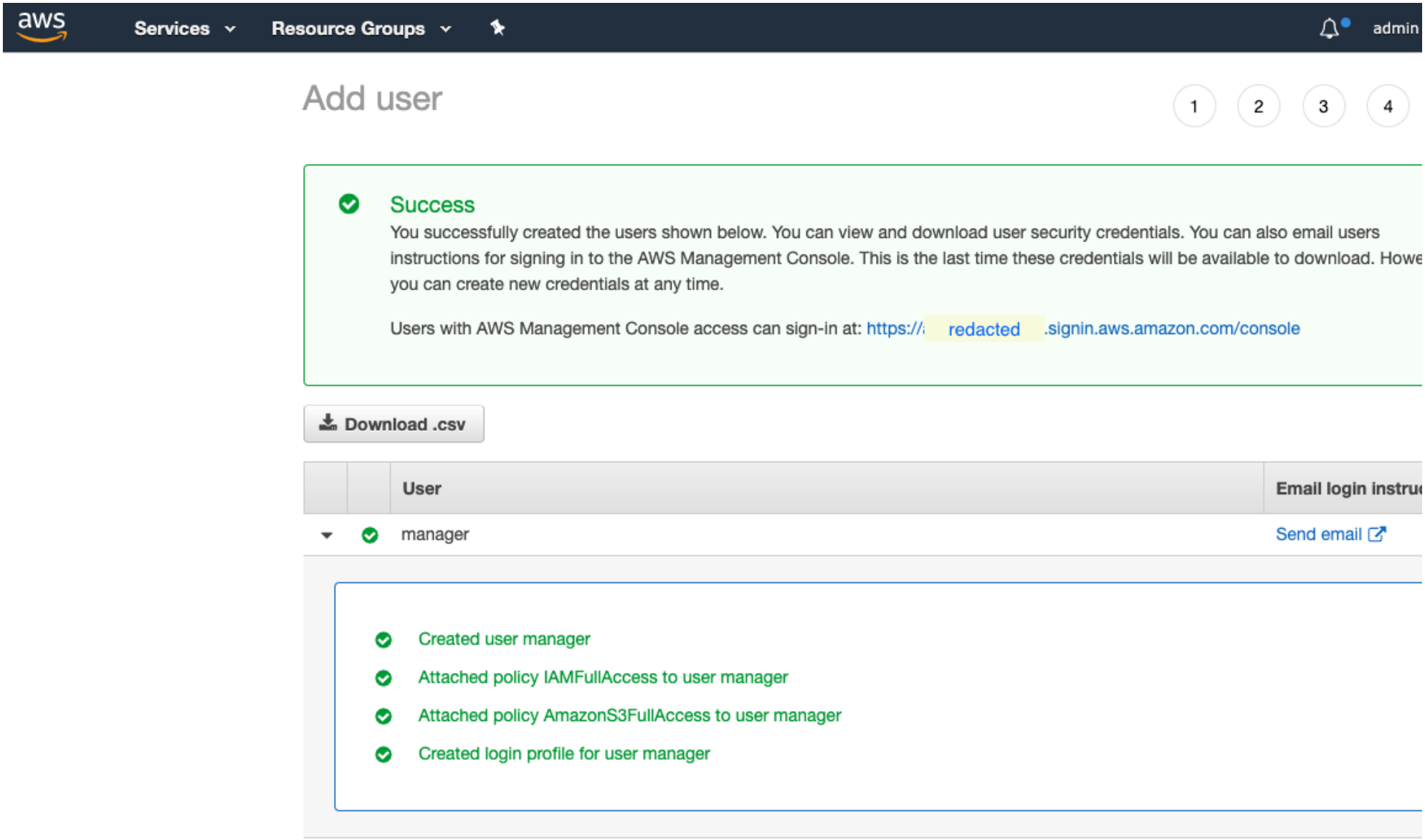
The following policies will be attached to the user shown above.

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



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

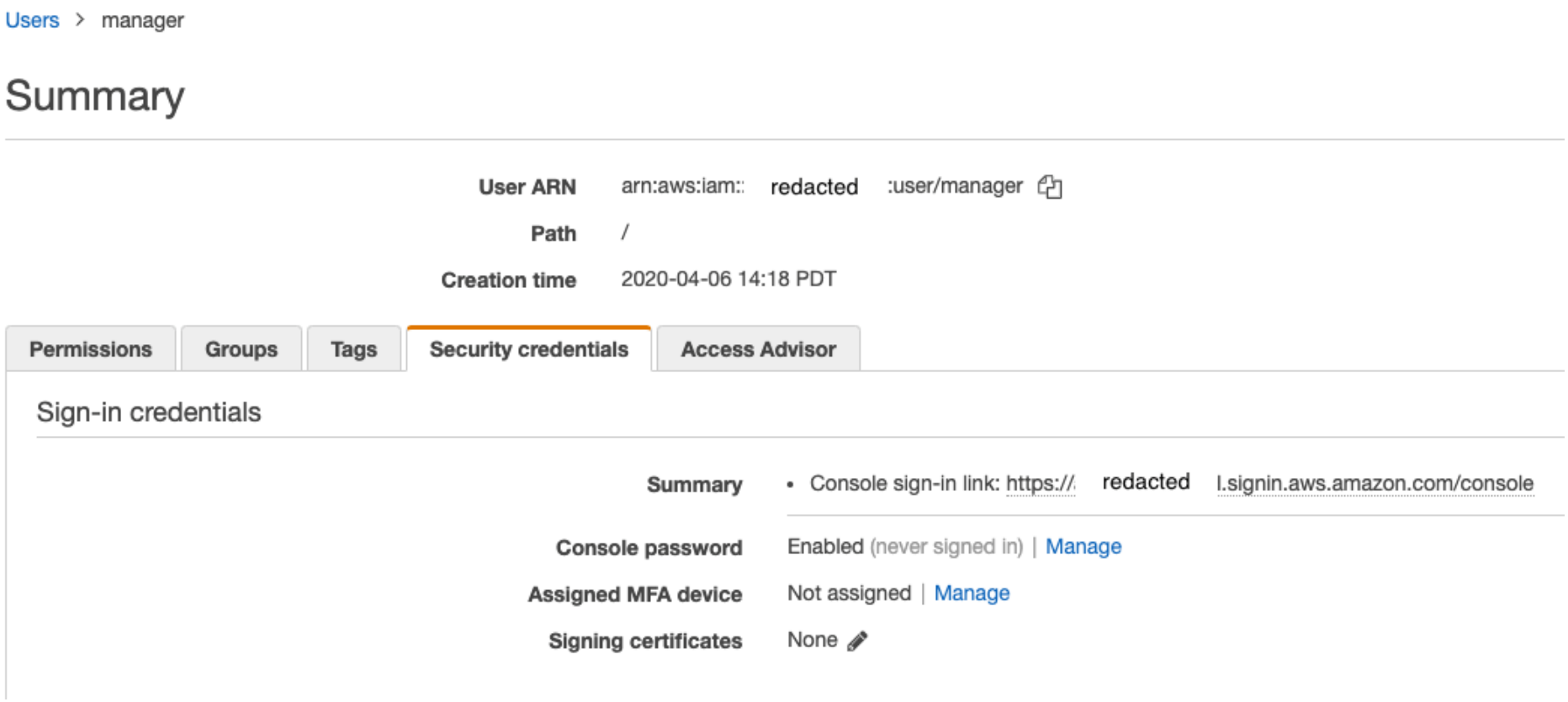
Exercise: Securing IAM User With MFA

Instructions

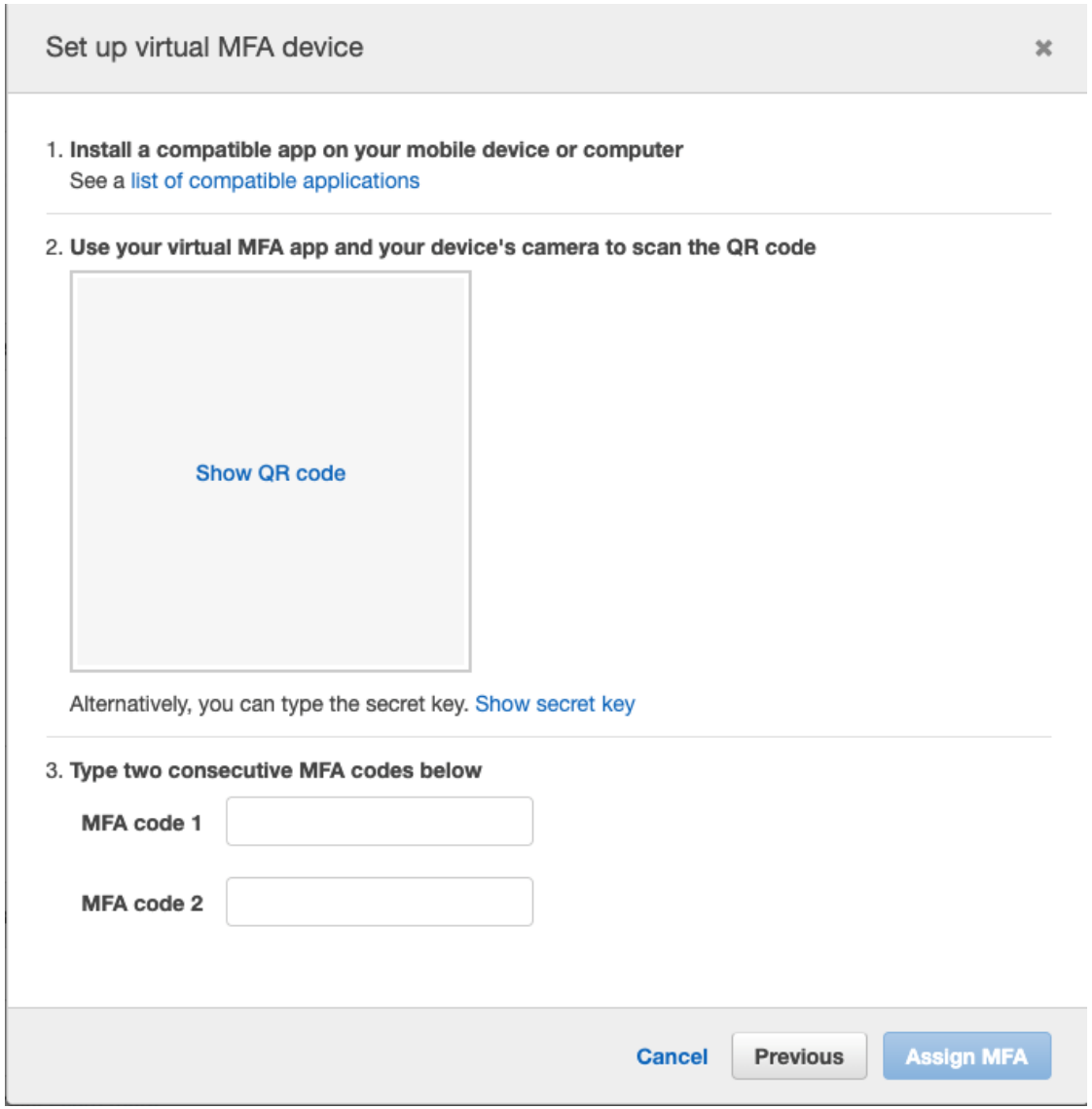
- If you have not yet done so, you must first create a **manager** AWS account
- Install an MFA app on your phone - the **Google Authenticator** app (Android, iOS) is a good choice
- Secure the manager account with MFA
- Log out and log back in to verify that MFA is enabled

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



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



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

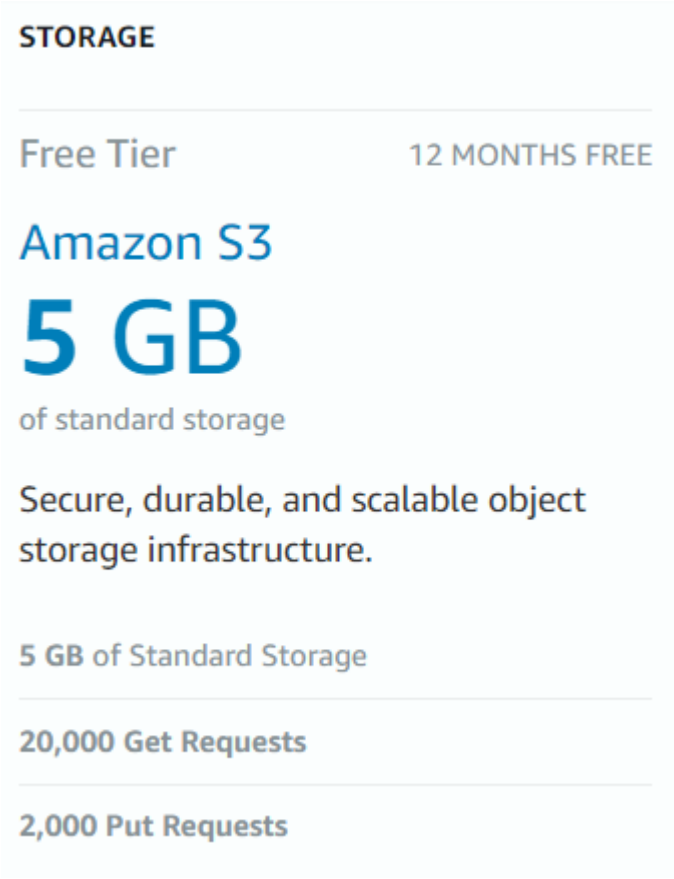
If you have not done so already, register with AWS and authenticate as the **manager** user

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

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

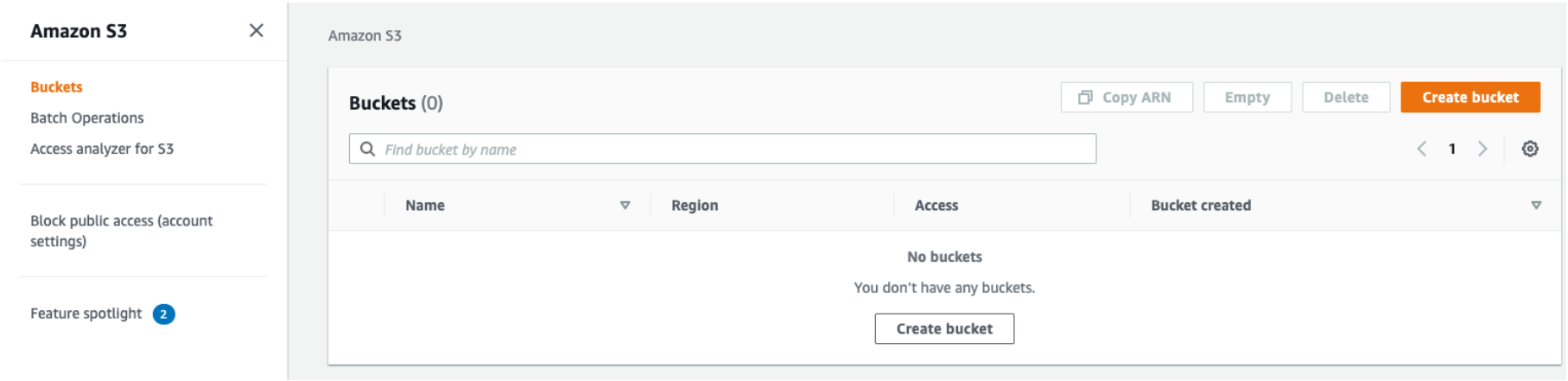
Upload content to both folders (a single file in each folder will suffice)

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.



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"

Amazon S3 > Create bucket

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

- [x] **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.

  - [x] **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.

  - [x] **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.

  - [x] **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.

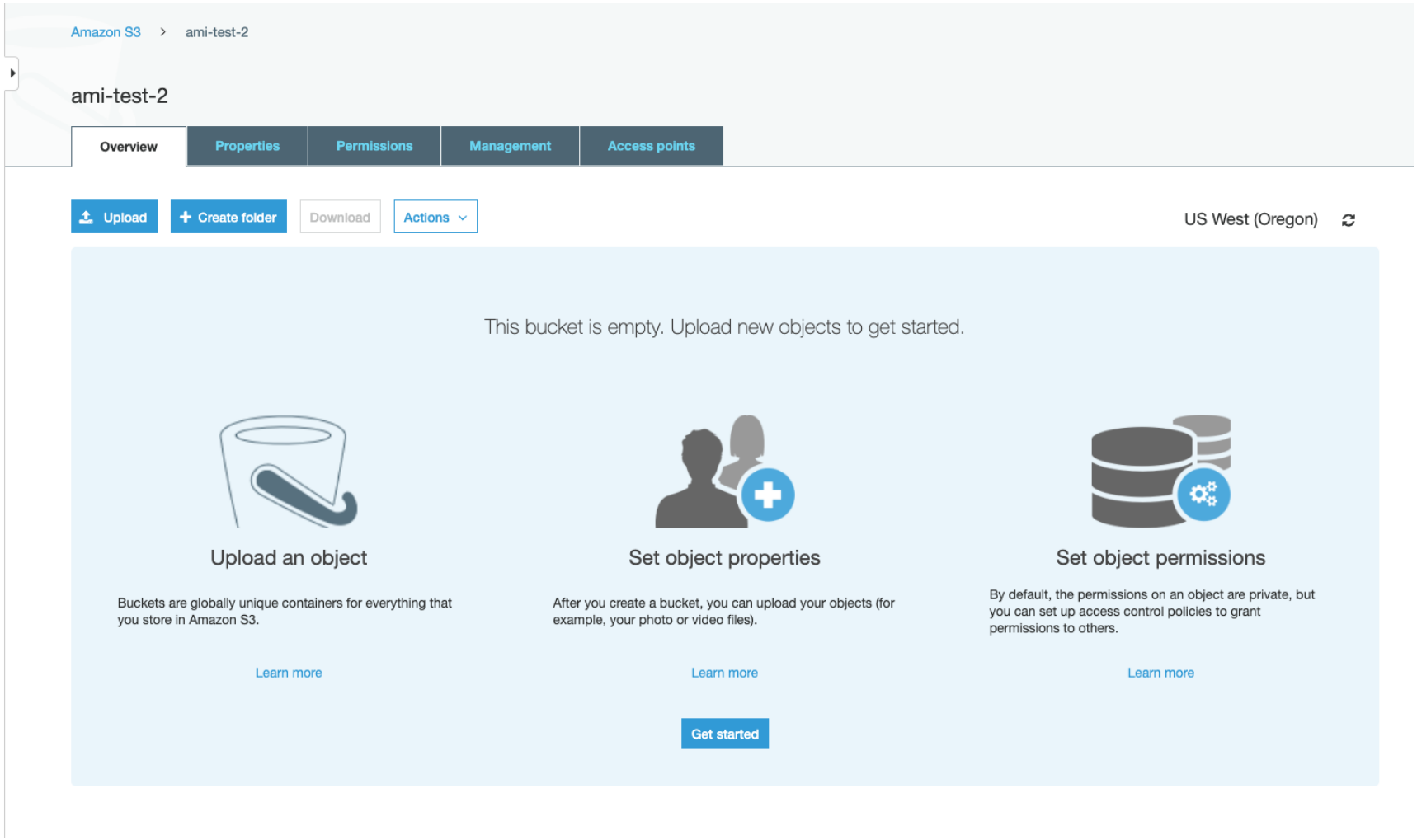
  - [x] **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

    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



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

Name | Last r

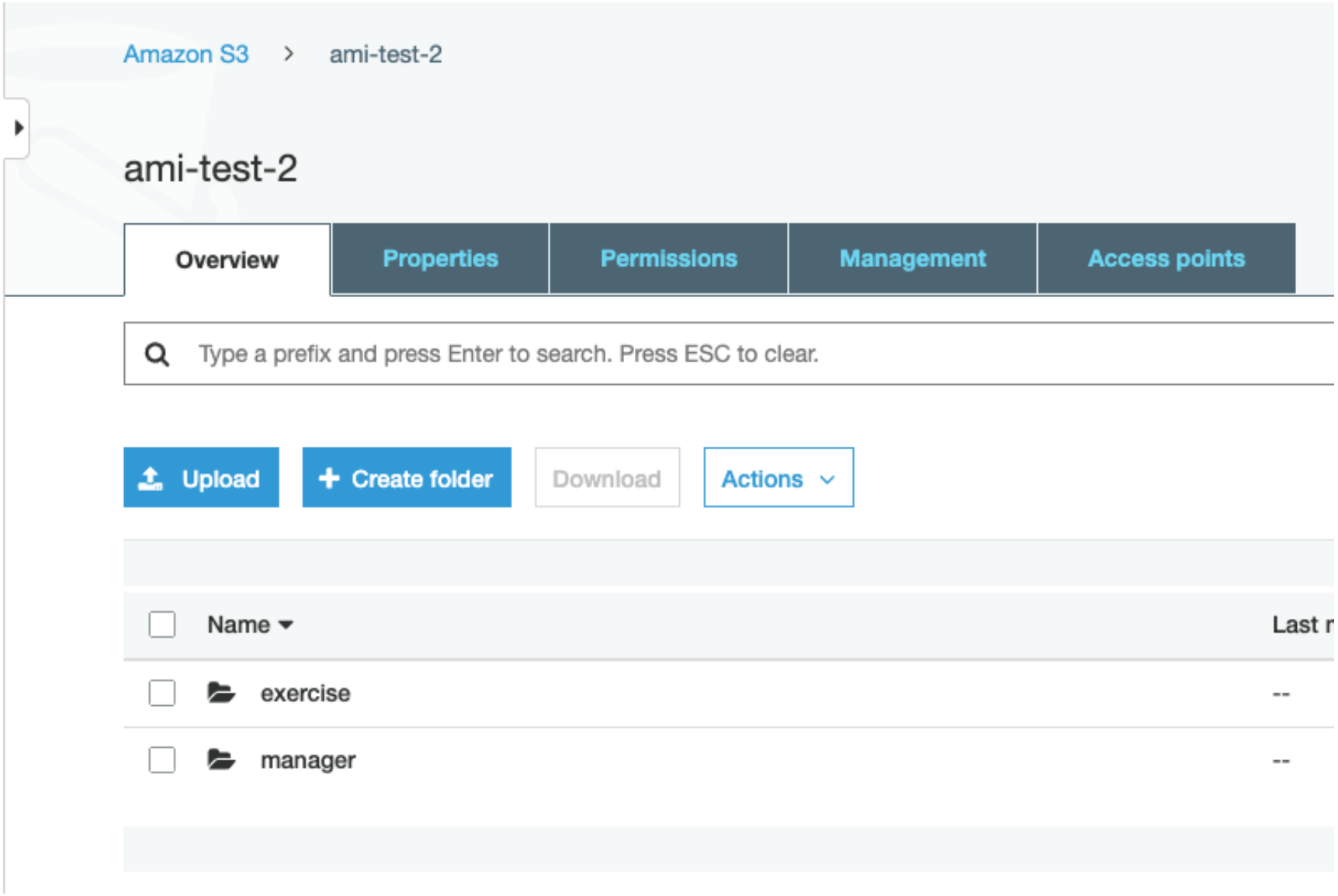
manager

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:

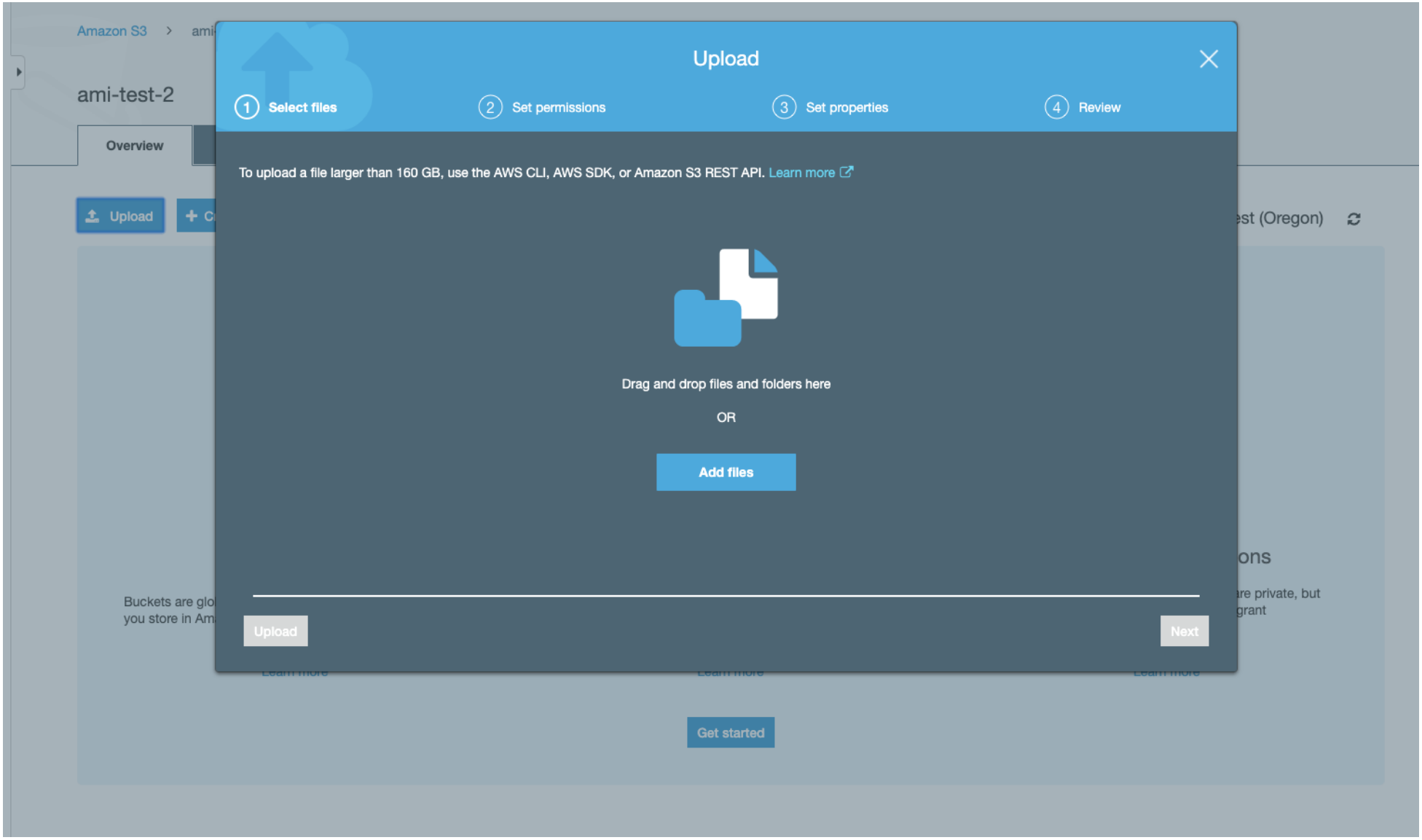
- (●) None (Use bucket settings)
- ( ) AES-256
  Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- ( ) AWS-KMS
  Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Save | Cancel

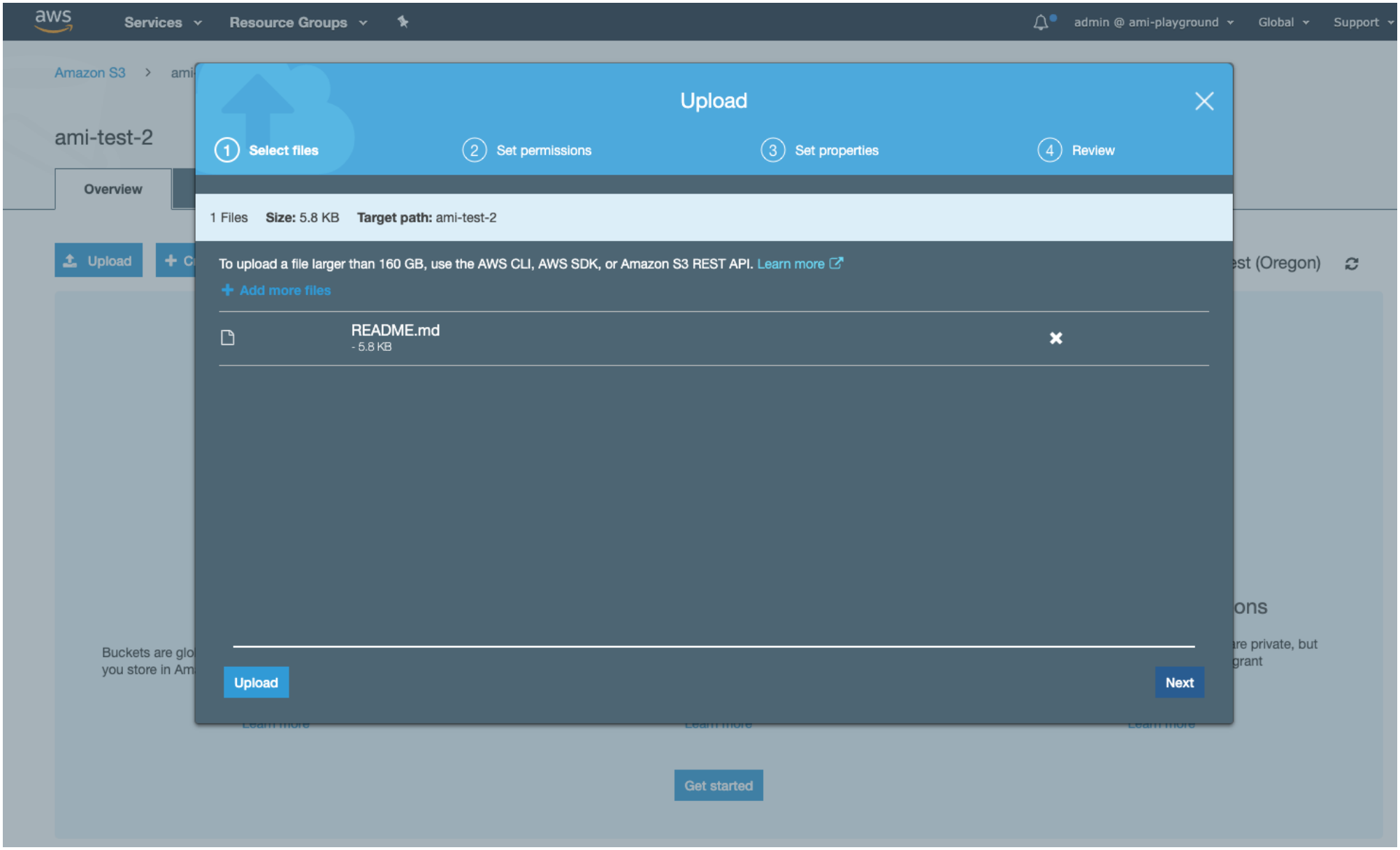
6. Create another folder called exercise



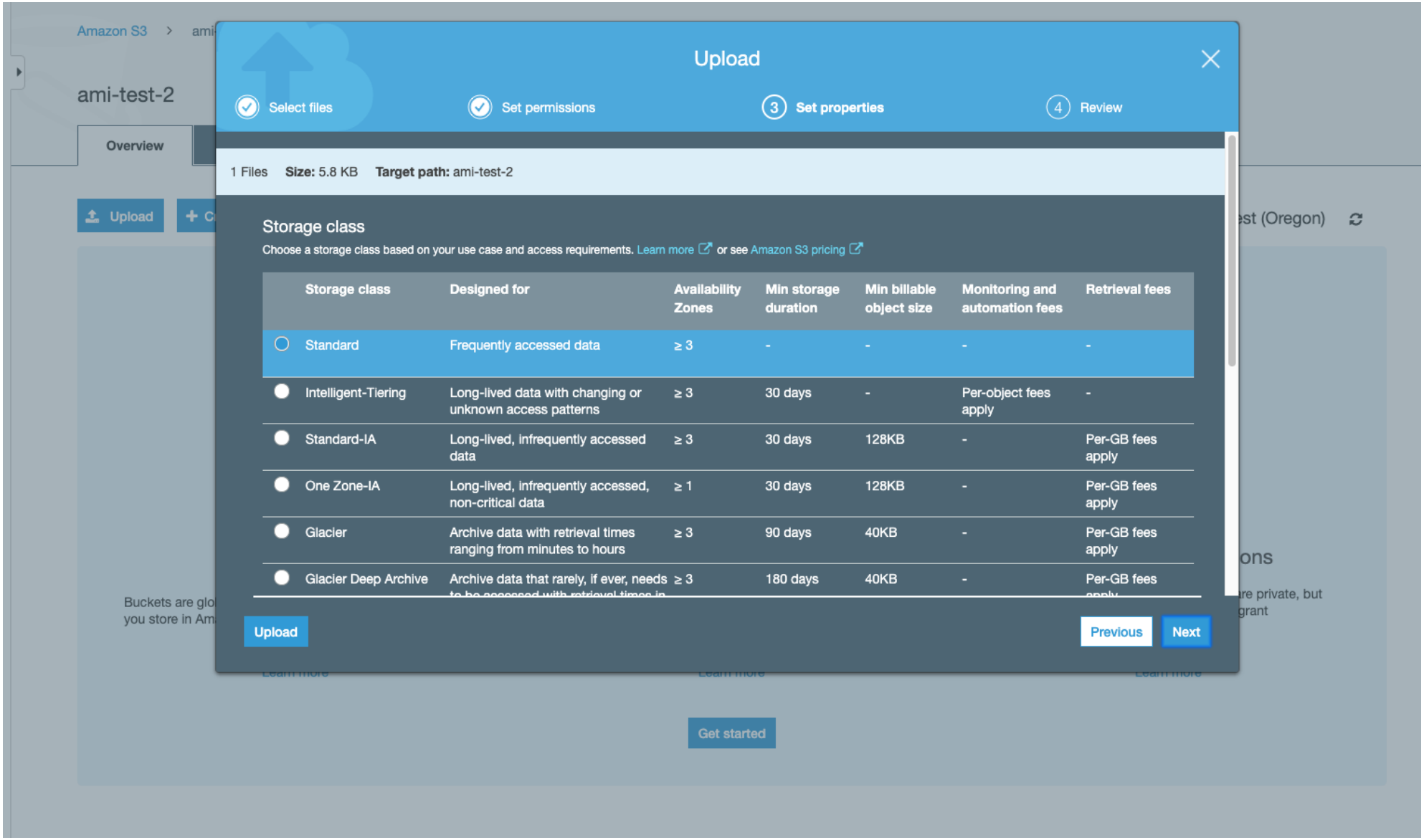
7. Click on the **exercise** folder to get into that folder
8. Click on the **Upload** button to upload a file (any file) into that folder



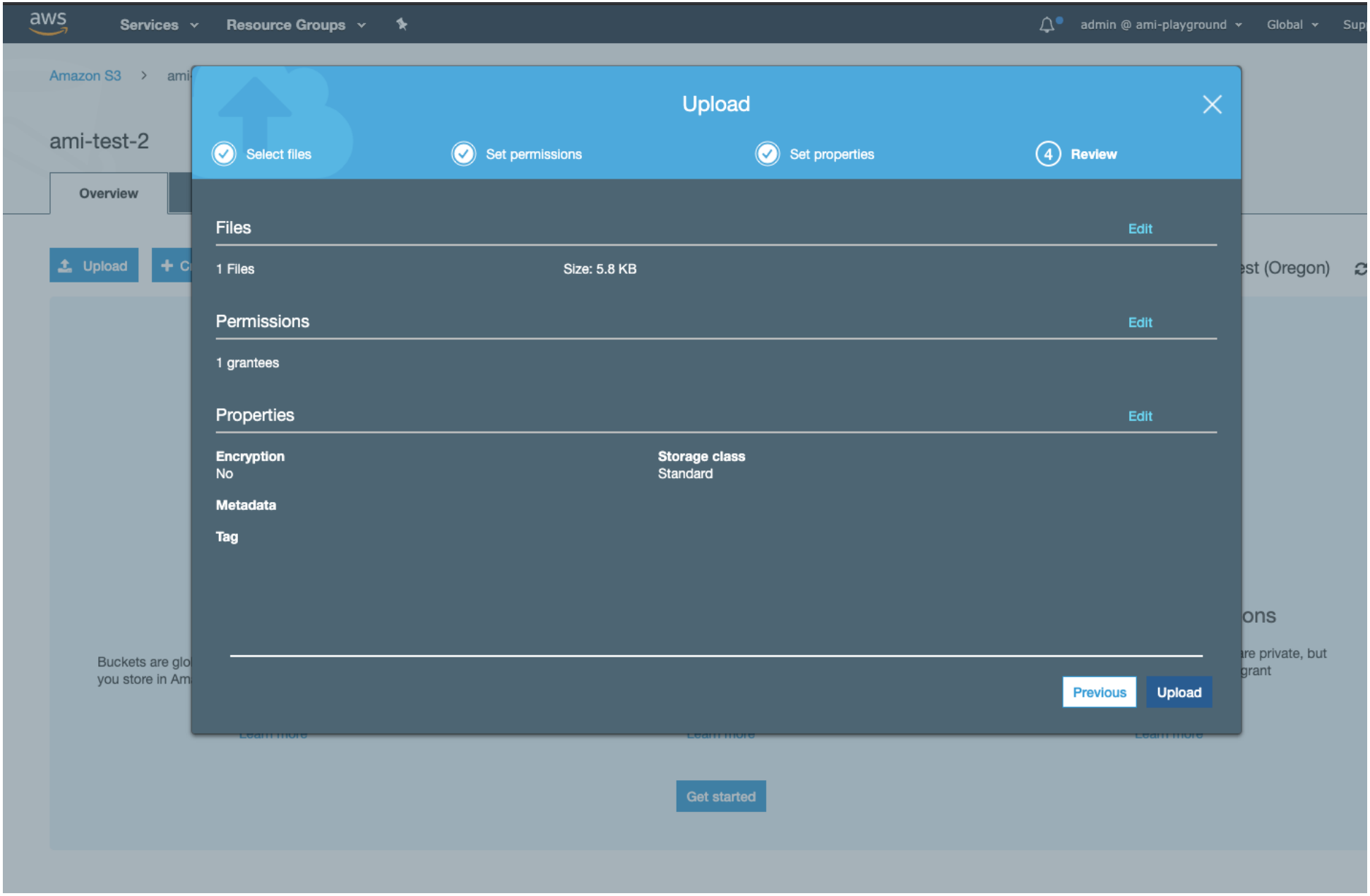
9. Either drag and drop a file onto the window or click the **Add files** button to start the upload process



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



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



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

US West (Oregon)

Viewing 1 to 1

Name	Last modified	Size	Storage class
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:

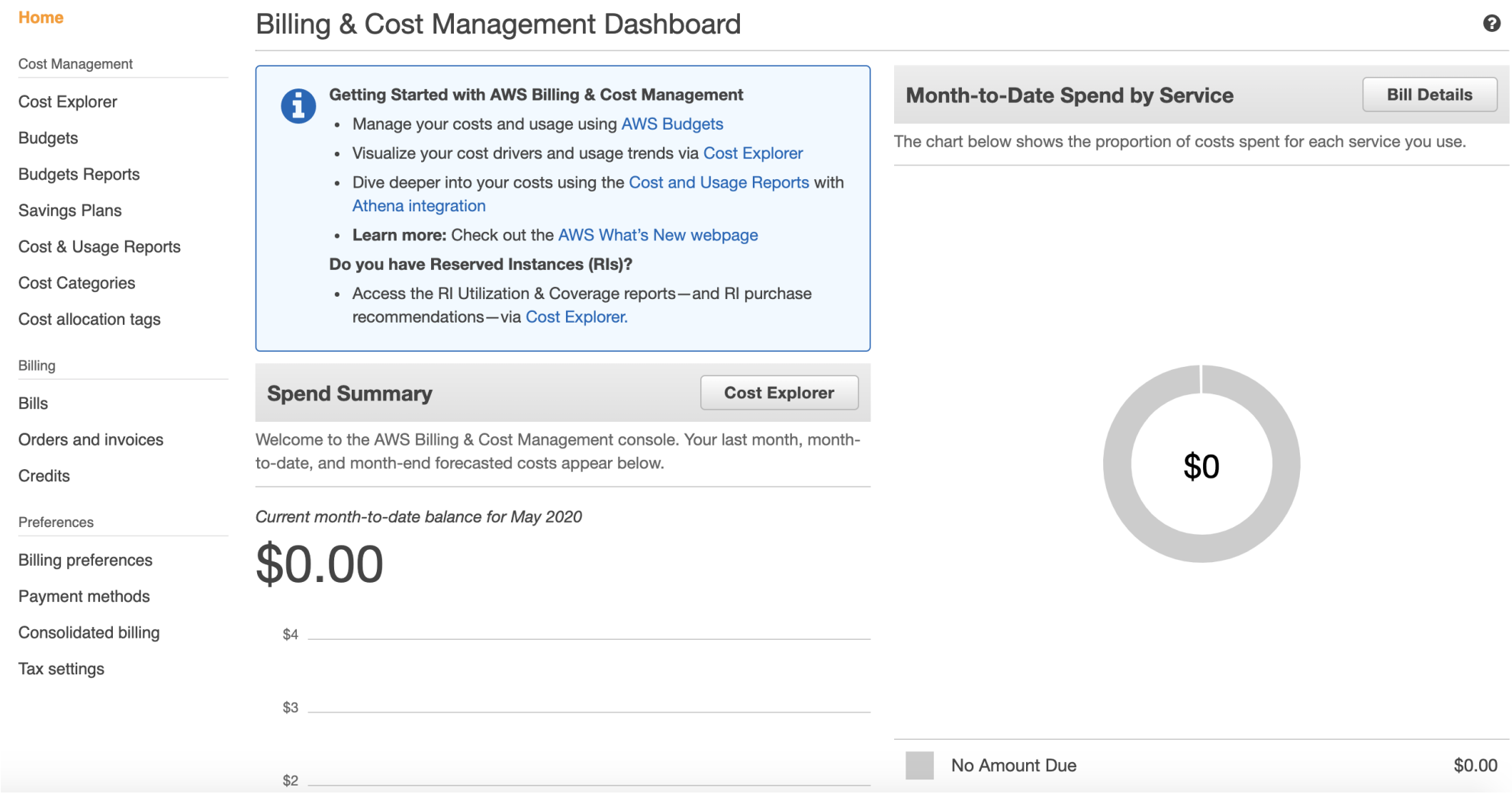
Step 1. Log into your AWS account.

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

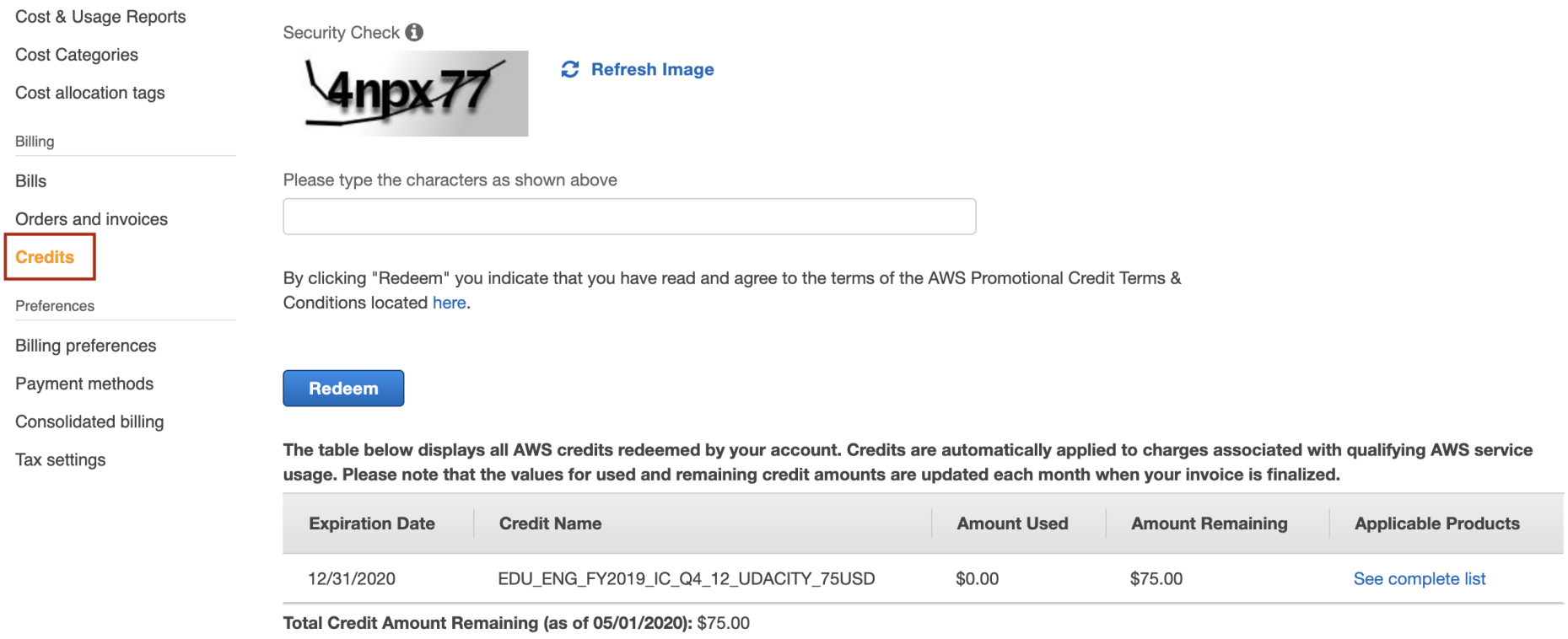


Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080

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.



AWS Elastic Compute Cloud (EC2)

- Resizeable, scalable compute capacity
- Instances 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

Intro to Cloud Computing https://www.udacity.com/course/intro-to-cloud-computing--ud080