SDEV Lab 0 – AWS Set-up

Overview: In this lab, you will set-up your AWS account, join AWS Educate as a UMUC institution member, and provide some baseline security for your root account that includes multi-factor authentication, the creation of a non-root user with admin privileges, and the establishment of a password policy.

To speed the process have the following items with you:

- Valid Credit Card
- Phone number that will be used to validate account
- Smart phone with Google Authenticator or similar Multi-Factor Authentication (MFA) software

Important Notes:

1. AWS is used for multiple SDEV Virtual Machine Labs. You may have completed this for another class already. If so, you can skip to end to see the deliverables required for sign-off on this exercise.
2. The screen captures for your session, may look different depending upon your Browser, and if AWS has changed its workflow. Use this as a guide, but realize your screens may look different but the end goals and results will be the same.
3. If you want to take advantage of the AWS educate grants, you must create an account using your UMUC student ".edu" account. If you don't, you will find much frustration associated with the AWS approval process. So, start out right away using the UMUC .edu account.
4. **Valid Credit Card Required:** If you follow the processes and recommendations in the course, you won't need to spend any of your money on AWS services. However; you will be asked for a credit card. If you apply for the AWS Educate account and only use the recommended services and types in this class, your credit card will never be charged. You should monitor your AWS account regularly to make sure you are aware of what is running and the charges, if any associated with that service.
5. **Start this on the first day of class or before.** Delays will impact your grade and successful completion of this course.

The high level steps include:

a. Creating a new AWS account for your UMUC student work.
b. Applying for the AWS Educate grant program as UMUC institution member.
c. Add Multi-factor Authentication to your root account.
d. Creating an Admin group within AWS.
e. Creating a user in AWS and assigning the user the Admin group permissions.
f. Creating a password policy for the users.
g. Documenting the process and confirming you are now an AWS Educate member. (Note: This gives you a $100 credit that is on top of the free tier 1 services you receive for a year under AWS)

Detailed steps with some screen captures and notes:

1. Open up your AWS account – Note this will be for your UMUC student AWS account

https://portal.aws.amazon.com/billing/signup#/start

As you create your student account, I recommend you use an account name such FirstnameLastnameUMUC (e.g. JamesRobertsonUMUC)

Also, be sure to **use your Student UMUC email**. This makes it easier to apply the AWS Educate grant funding. In fact, if you don't, you will be seriously delayed in receiving your grant from AWS. You will need to select the Continue button and complete the remaining validation process to create your account. See figure 1.

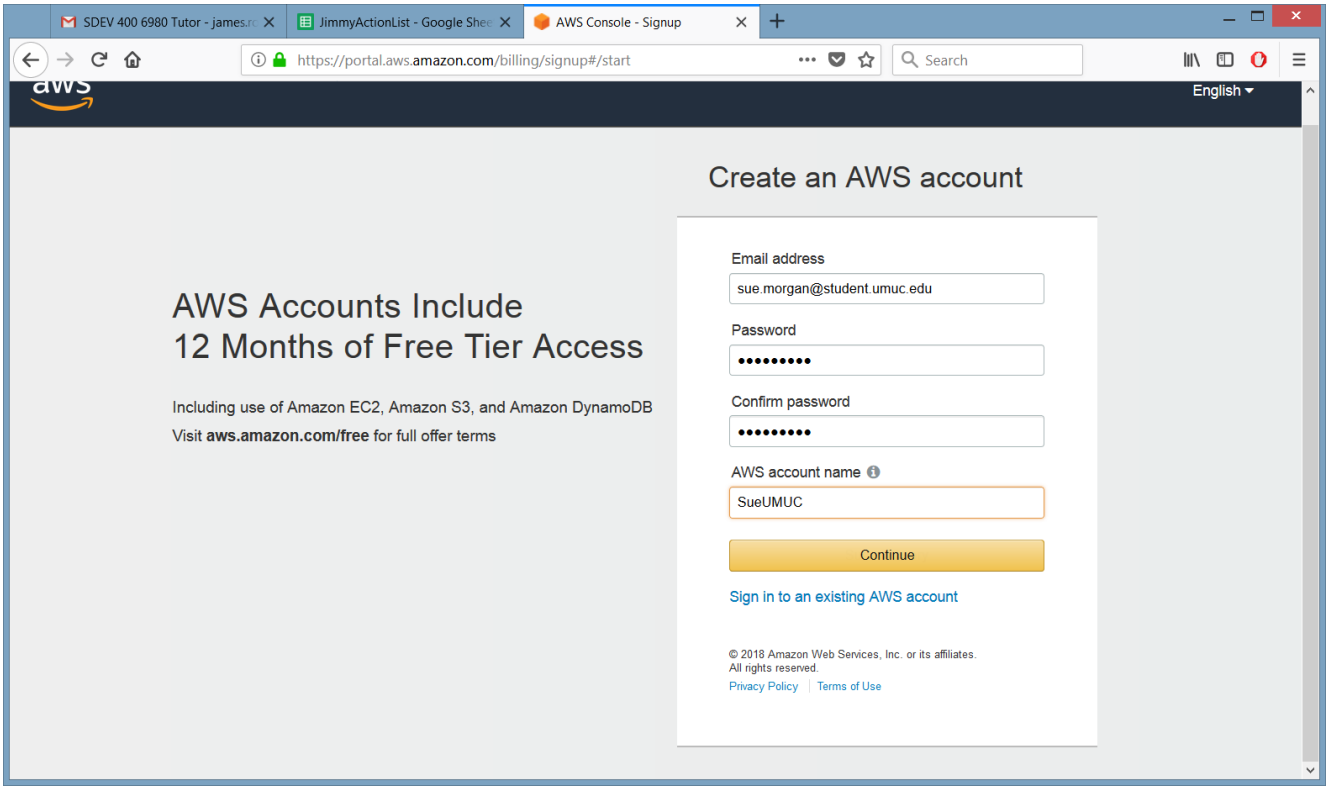

Figure 1 Creating a New AWS Account

Select Personal as the account type, fill in all required fields and then select "create account and continue." See figure 2.

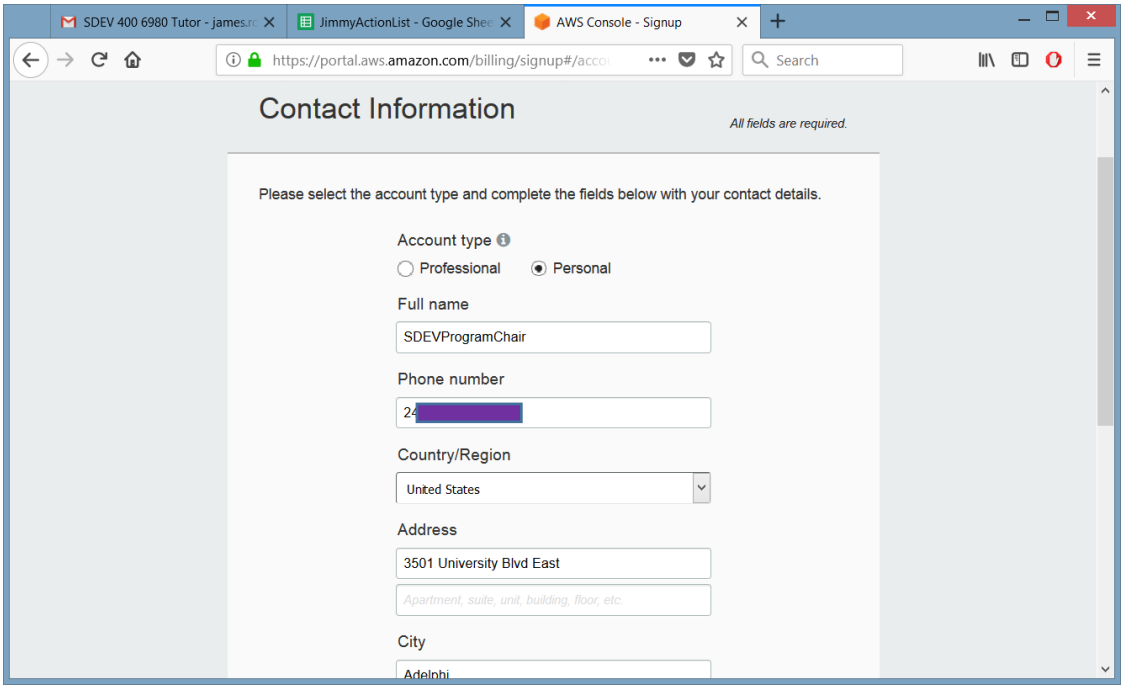

Figure 2 Account Type Fields

Enter your valid credit information to continue. This is required to create an account with AWS. Click "secure submit" to continue. (See figure 3)

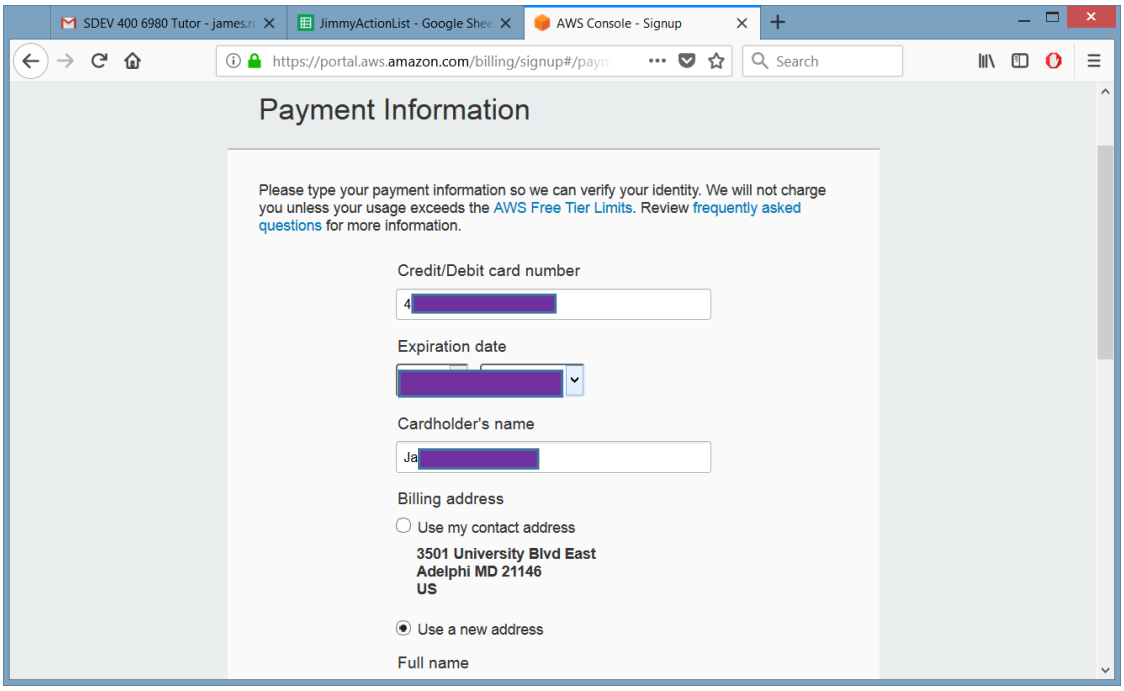

Figure 3 Enter Valid Credit Card Information

As shown in figure 4, enter phone verification which is also required.

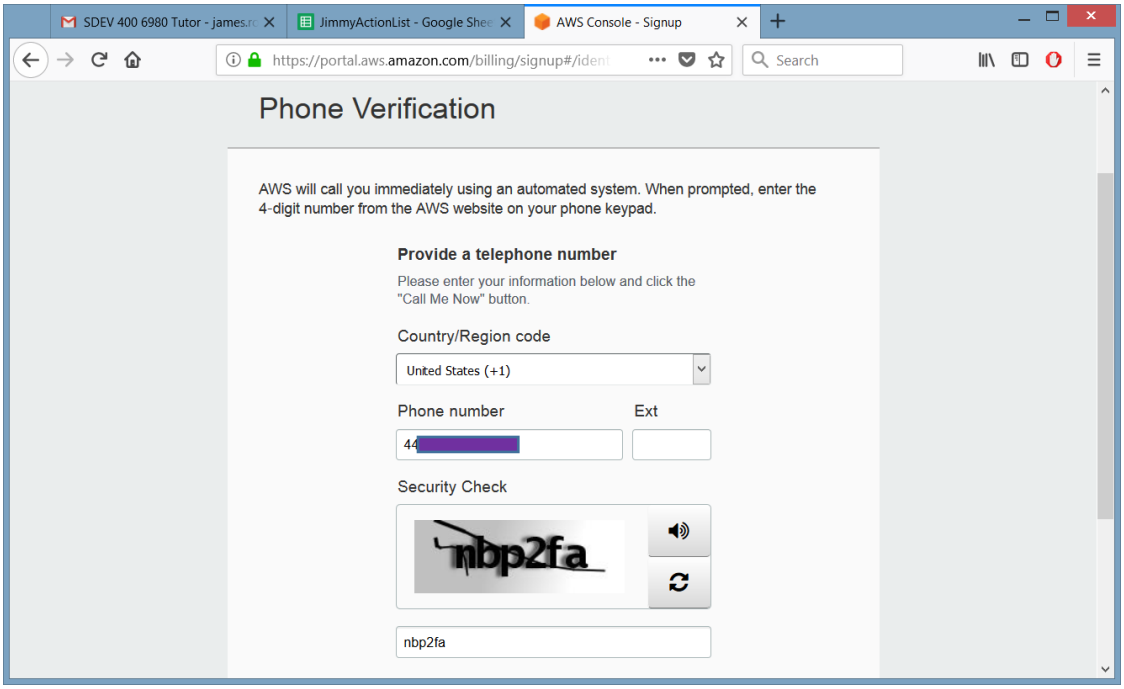

Figure 4 Validate Account with Phone Number

You will be called on the phone you provided and then given a 4-digit pin to enter. Once successful, you will receive be asked to click continue as shown in Figure 5.

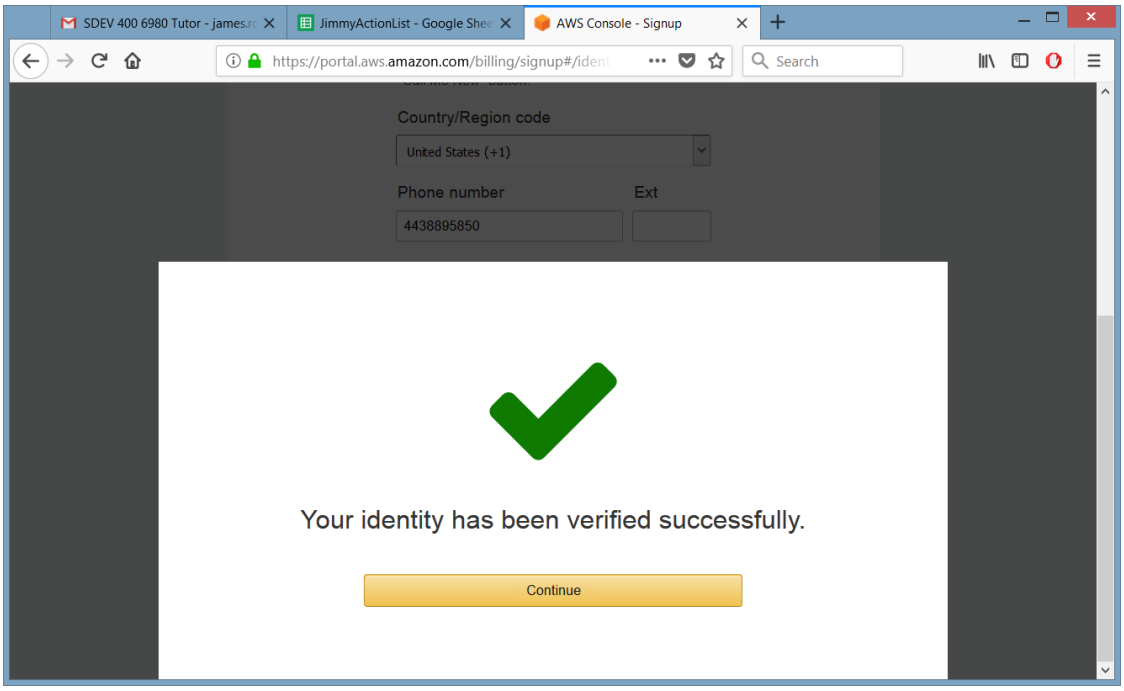

Figure 5 Identity verified

Select the basic plan (free) to continue.

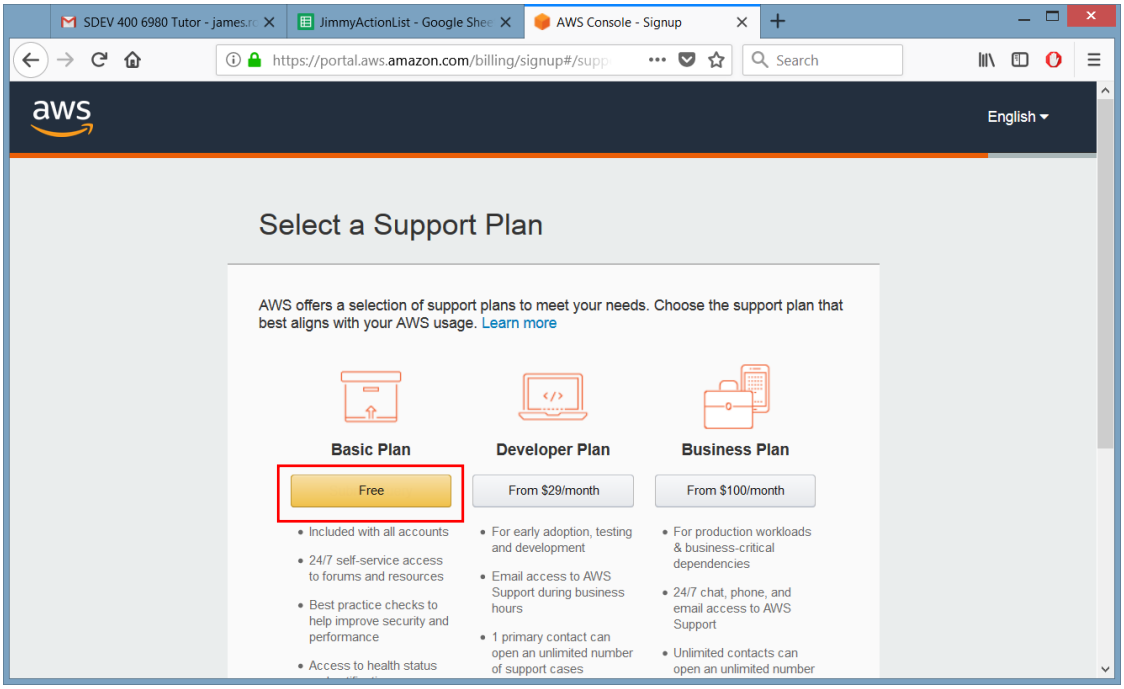

Figure 6 Select the Basic Support Plan

Next, click “Sign in to the console” to continue as shown in figure 7.

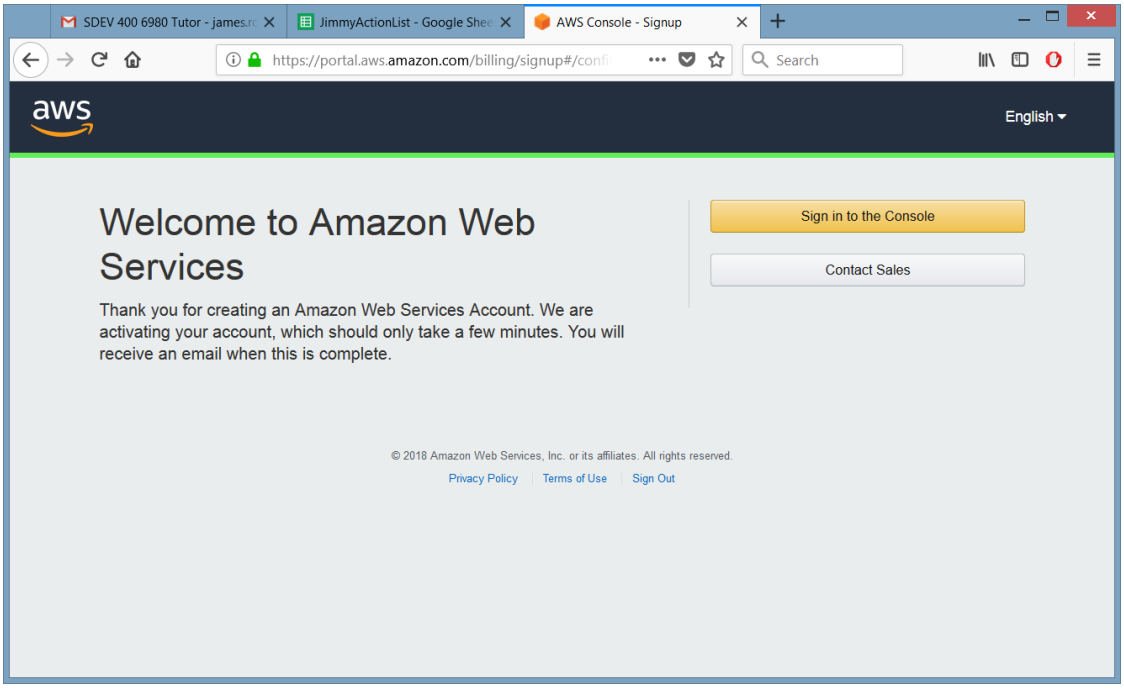

Figure 7 Sign in to the Console

Be sure to record your **12-digit AWS account ID**. You will need this to create your AWS educate account in the next step. To sign-in click on “Sign-in using root account credentials”. (See figure 8)

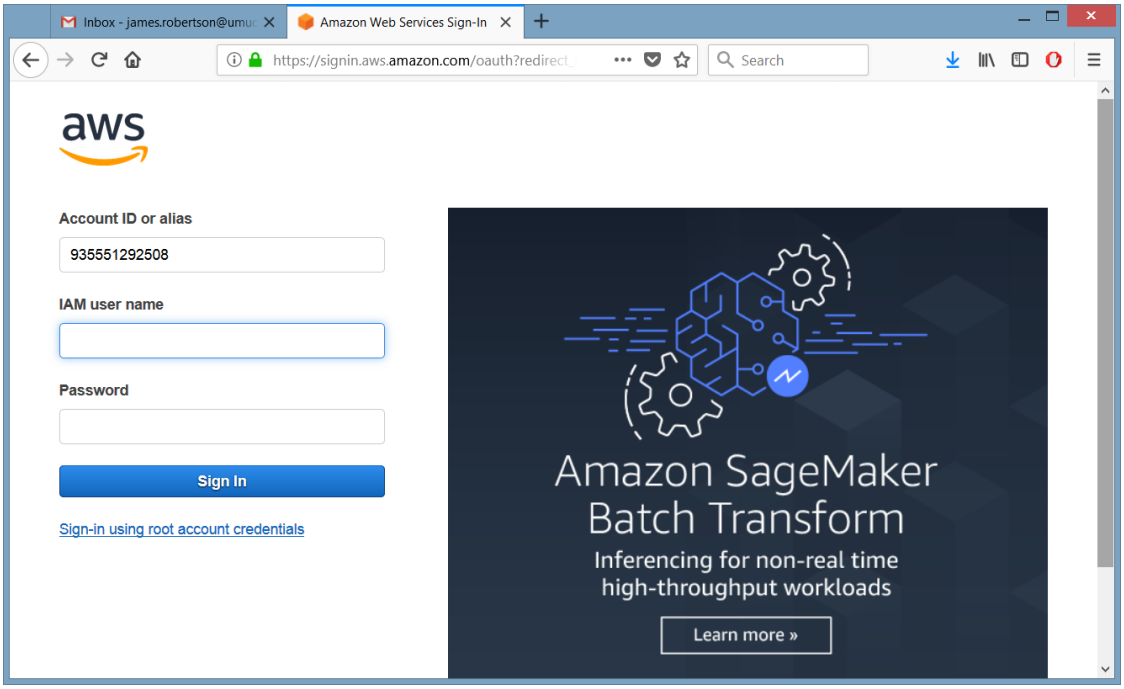

Figure 8 Sign-in using root account

Enter your email address and password you originally set-up when you created the account and you now have access to AWS using your root account. (See figure 9).

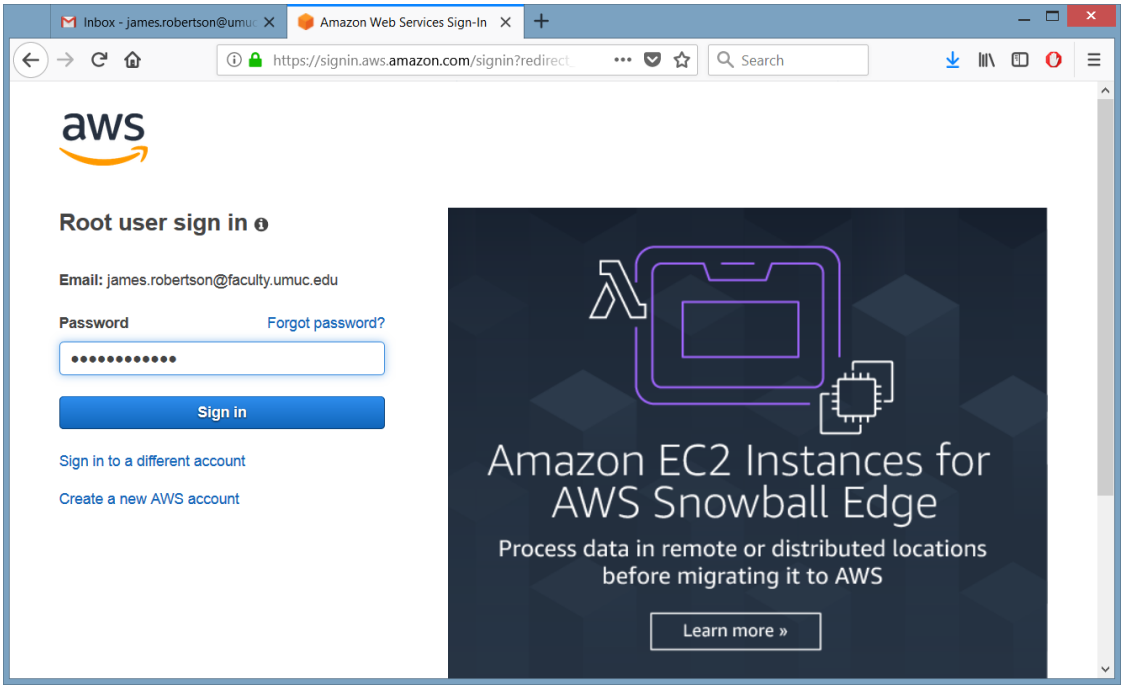

Figure 9 Enter Root Credentials

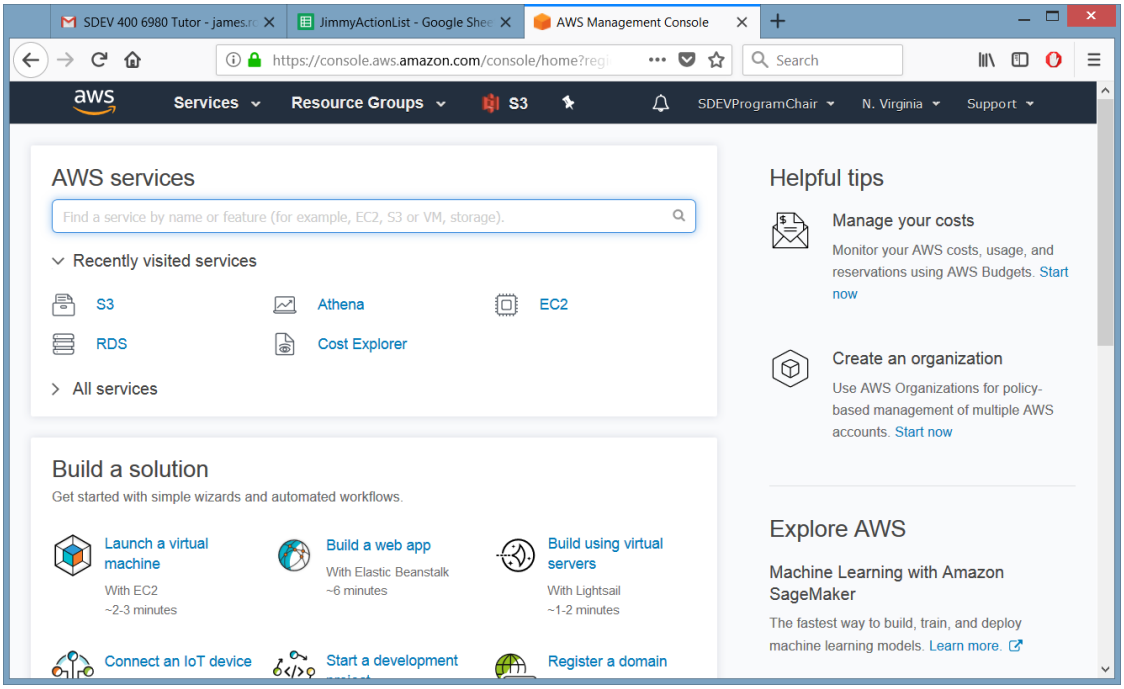

Figure 10 Successful AWS Login

Now that you can successfully login, the following steps provide details on applying for an AWS Educate grant and securing your account. You should not use your root account for day-to-day operations. These steps provide that security as well as lock down to protect your root account.

2. Apply for an AWS Educate account using this URL:

   https://aws.amazon.com/education/awseducate/

Figure 11 shows a current version of the AWS Educate sign-in page. Click the "Join AWS Educate" button to continue.

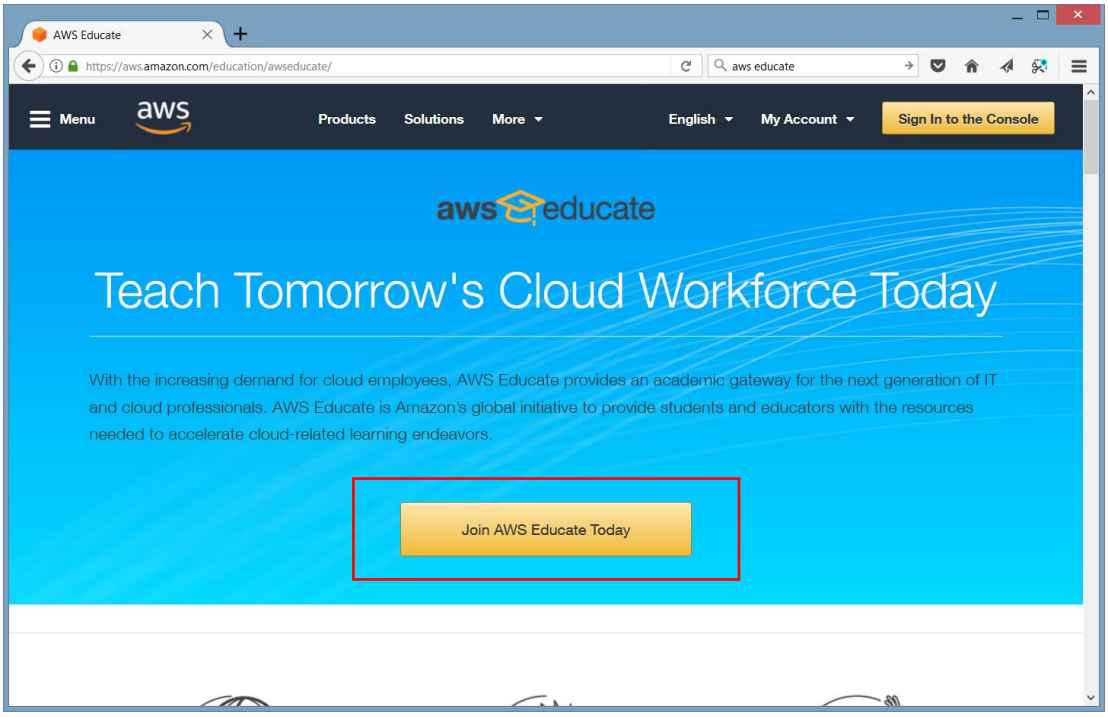

Figure 11 Joining AWS Educate

As shown in figure 12, select the Student role to continue.

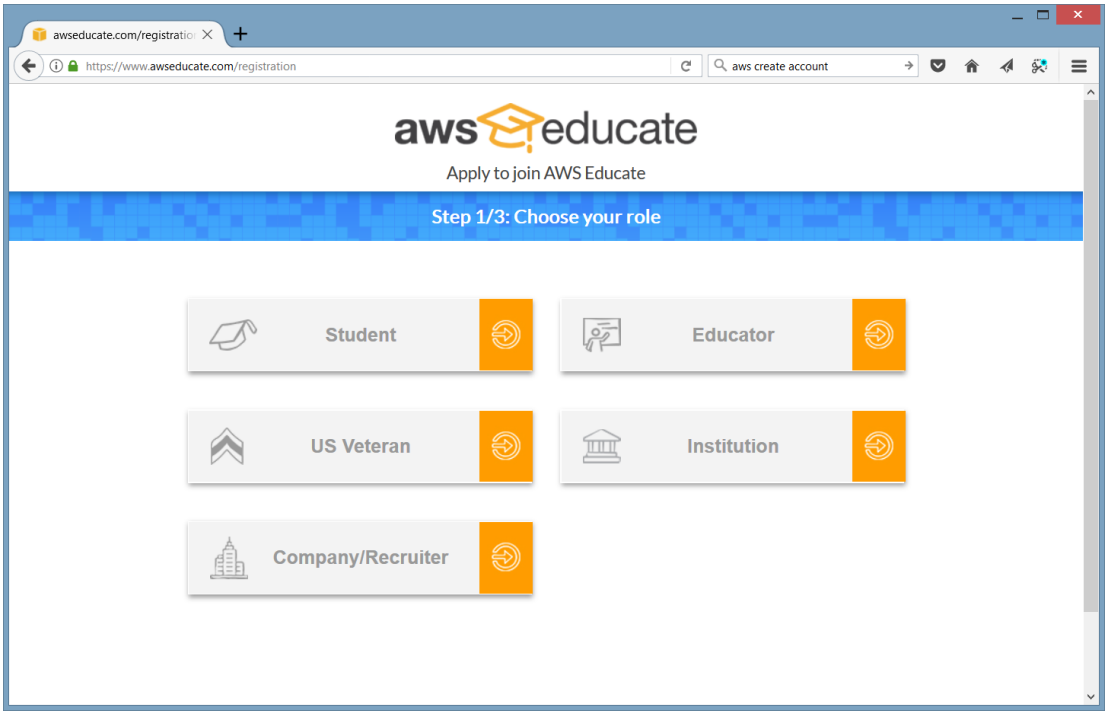

Figure 12 Select the Student Role

Be sure to enter University of Maryland, University College for the school as you will receive additional credits to use as UMUC is AWS Educate member. As shown in figure 13, be sure to fill in all require information and select "Next" to complete the forms.

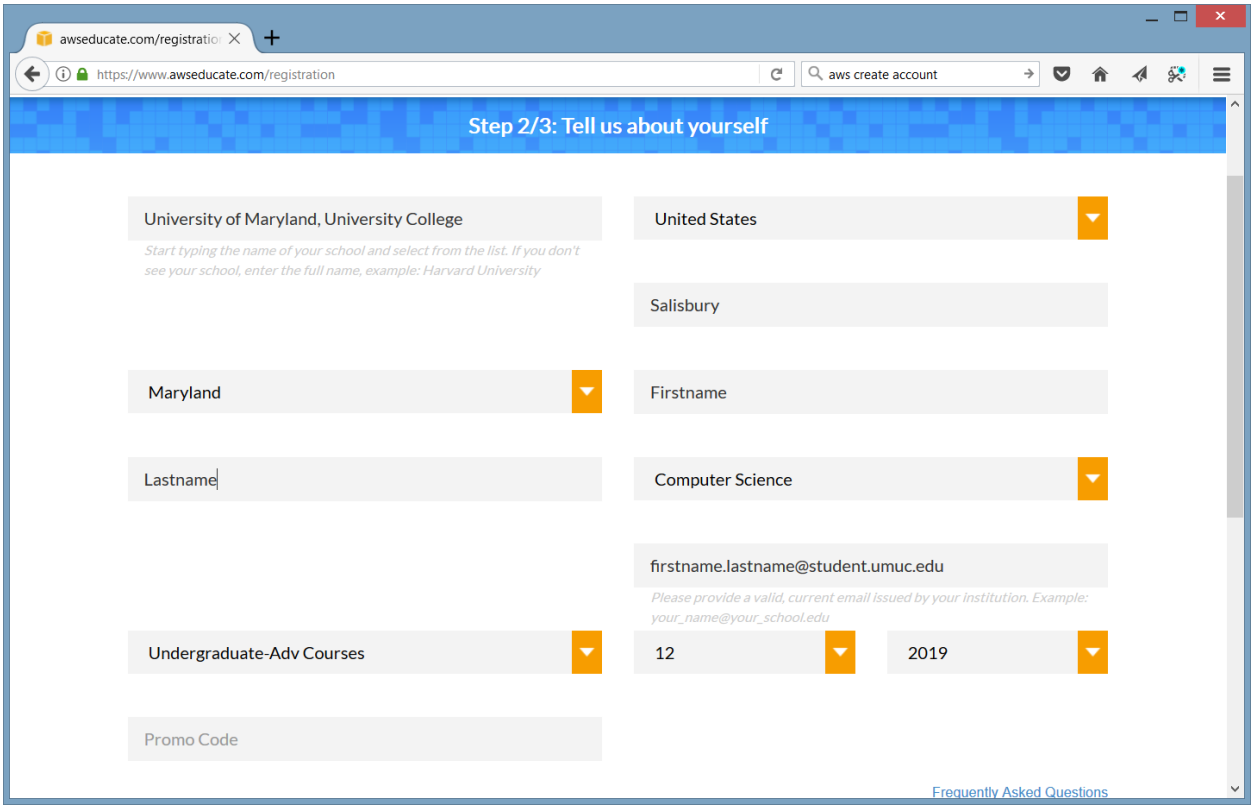

Figure 13 Complete the AWS Educate Form

After you have completed the AWS Educate application, you will receive an email from AWS saying they are reviewing your application. Typically this occurs within 3 business days or sooner. Therefore, be sure to start this request as soon as possible. Figure 14 shows an email similar to what you will initially receive.

Hi James,

Thank you for applying for AWS Educate. We have received your application, and it is currently under review. You will receive an email once the review is complete.

If you have any questions, please click here to contact AWS Educate support.

Thank You!
The AWS Educate Team

Figure 14 AWS Educate Initial Email

While awaiting your approval, you can login into AWS with your root account and set-up some baseline security. The steps for this are:

3. Login with your username and password you set-up when you created your AWS account.

The AWS URL sign-in is typically found at this URL. The URL will change once you create a non-root to sign-in

https://aws.amazon.com/console/

As shown in figure 15, click sign in to the console to proceed. Note, you should sign-in via root user account (typically your email you used when you created your AWS Account) for your first session.

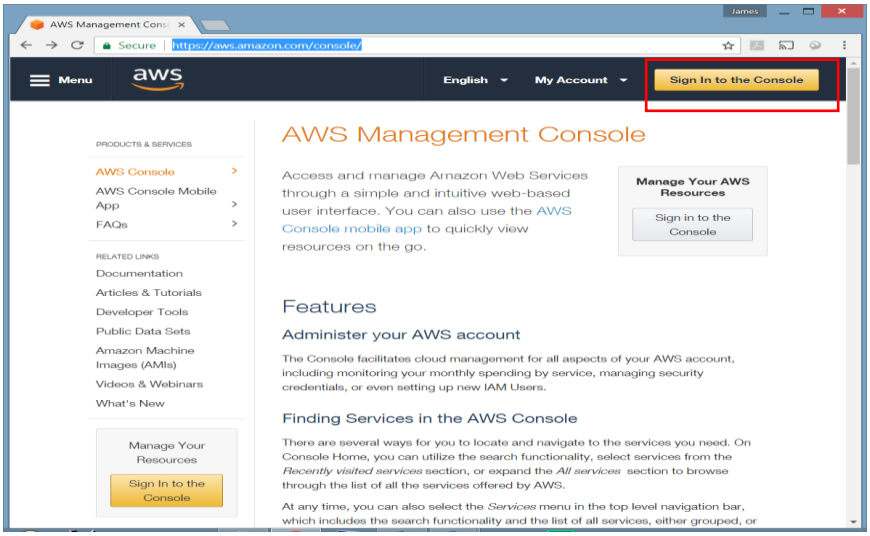

Figure 15 Sign In to the AWS Console

As shown in figure 16, enter your AWS root account password to continue with the login.

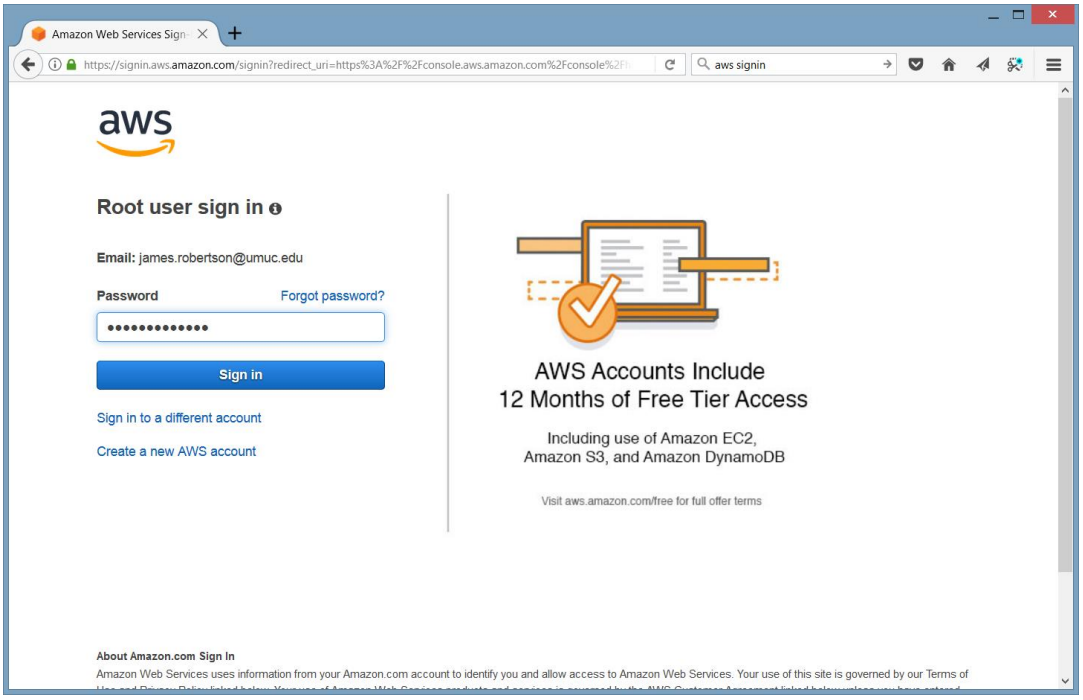

Figure 16 Enter your Root login password

4. Once connected, you should go to the Identify and Access Management (IAM) Dashboard and perform all of the steps for securing your account including: Deleting root access keys (which happens by default), activating MFA on your root account, Create an Individual IAM user, Use groups to assign permissions, and apply an IAM password policy.

As shown in figure 17, the IAM screen will look initially look similar to the screen capture below.

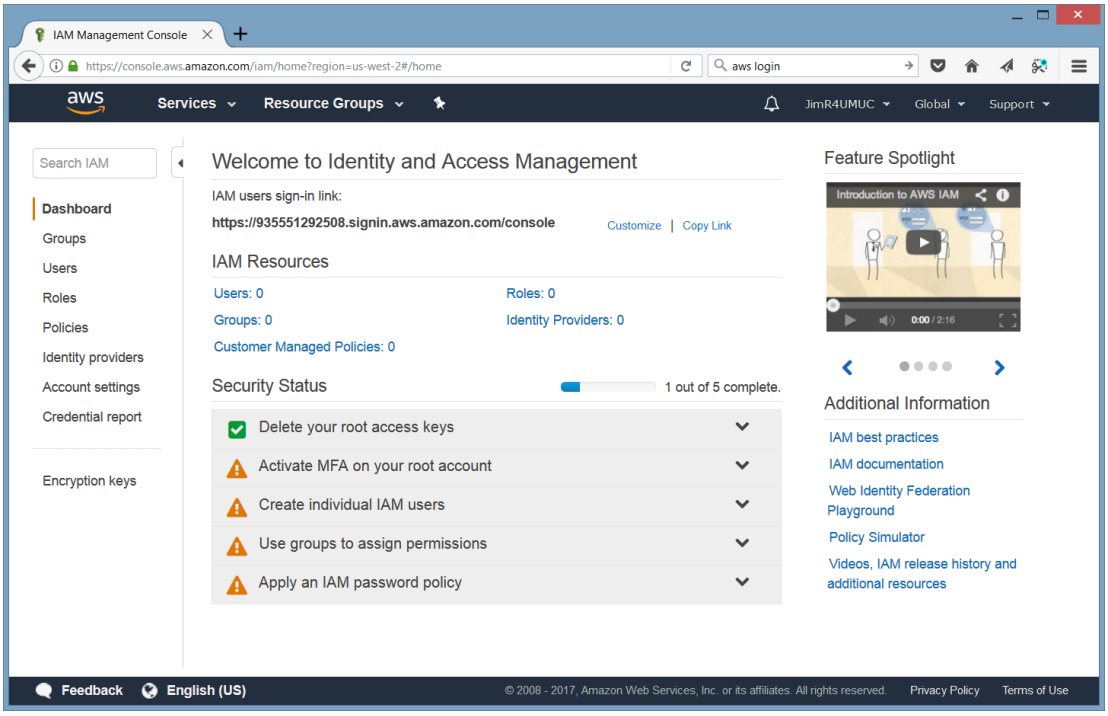

Figure 17 IAM Initial view

It is a cloud security best practice to not use your root account for routine access. By default, this account will not have any access keys generated. You should also activate Multi-Factor Authentication (MFA) on the root account for an extra security measure. If you have a smart phone, you can install the google authenticator app (this runs on Apple and Android devices) for a virtual MFA device.

Be sure to install the Google Authenticator on your smart phone before proceeding to the next steps. You can download the Google Authenticator app from your smart phone app store.

Clicking on the Activate MFA on your IAM account will expose the Manage MFA functionality as shown in figure 18.

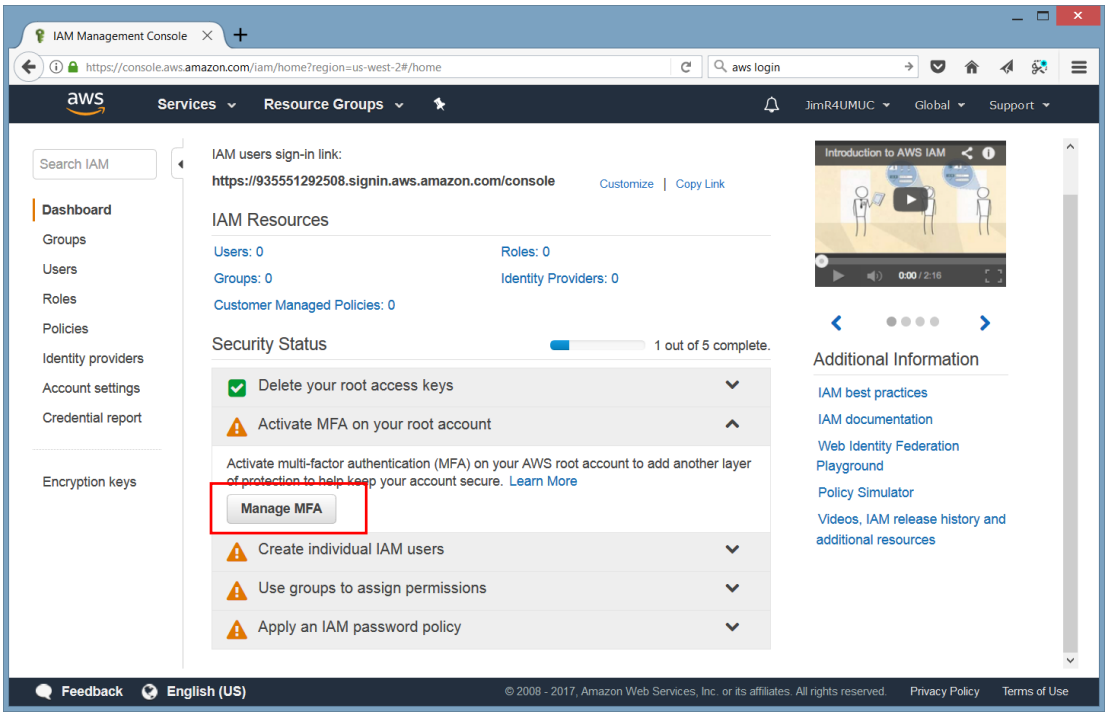

Figure 18 Implementing MFA

Click on the Manage MFA and then select Virtual MFA Device and then select “Next Step” as shown in figure 19.

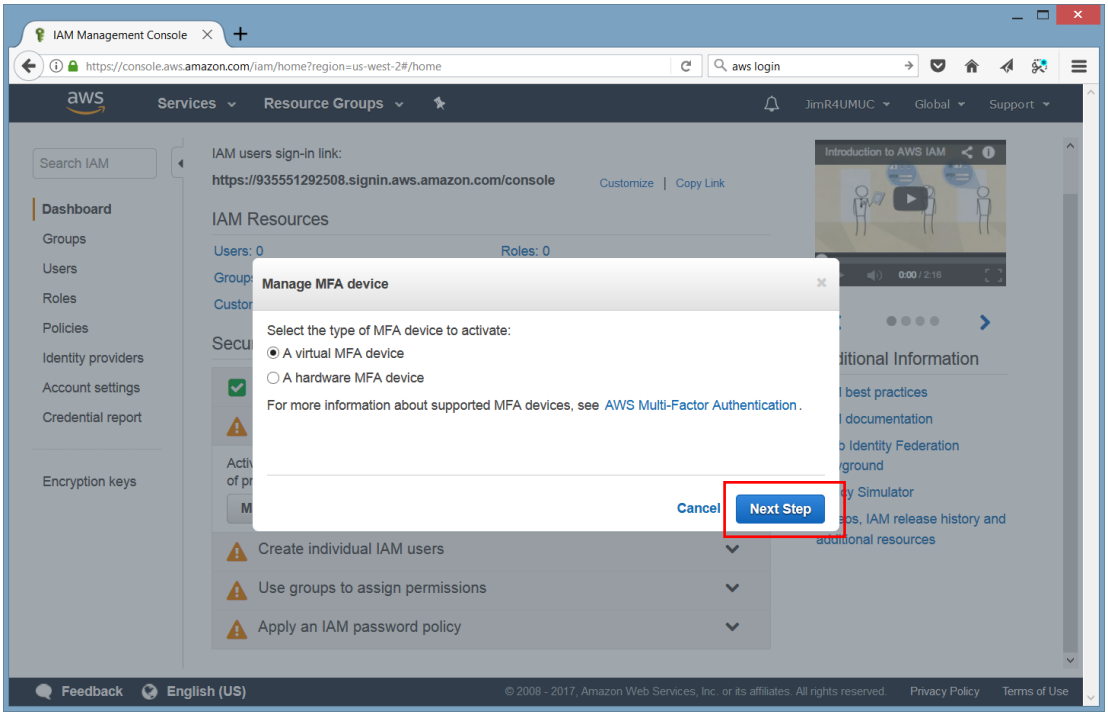

Figure 19 Selecting Virtual Device

As you click through the next steps, you will be asked to scan the code with your smart phone. (You can enter it manually as well.) Figure 20 shows the request to enter two subsequent authentication codes from your authenticator app from your smart phone. To proceed, capture two consecutive 6-digit codes from the smart phone and enter them. (Do not place spaces between the 3-digit sets of numbers) They should be entered without any spaces.

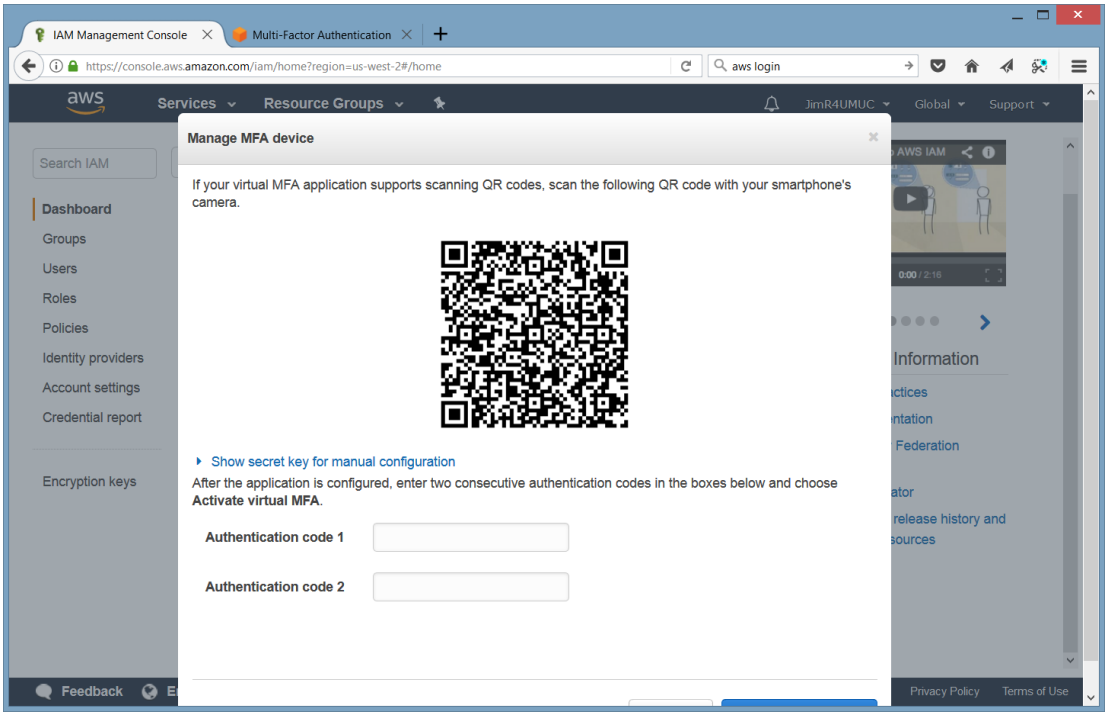

Figure 20 Entering Authentication Codes

To test the MFA, logout of your AWS root account, then log back in. After you enter your password you will be prompted to enter an authentication code. Be sure you have your smart phone with you to read the 6-digit authentication code and enter it to successfully login into the system. Figure 21 demonstrates the screen you may see to enter your 6-digit authentication code.

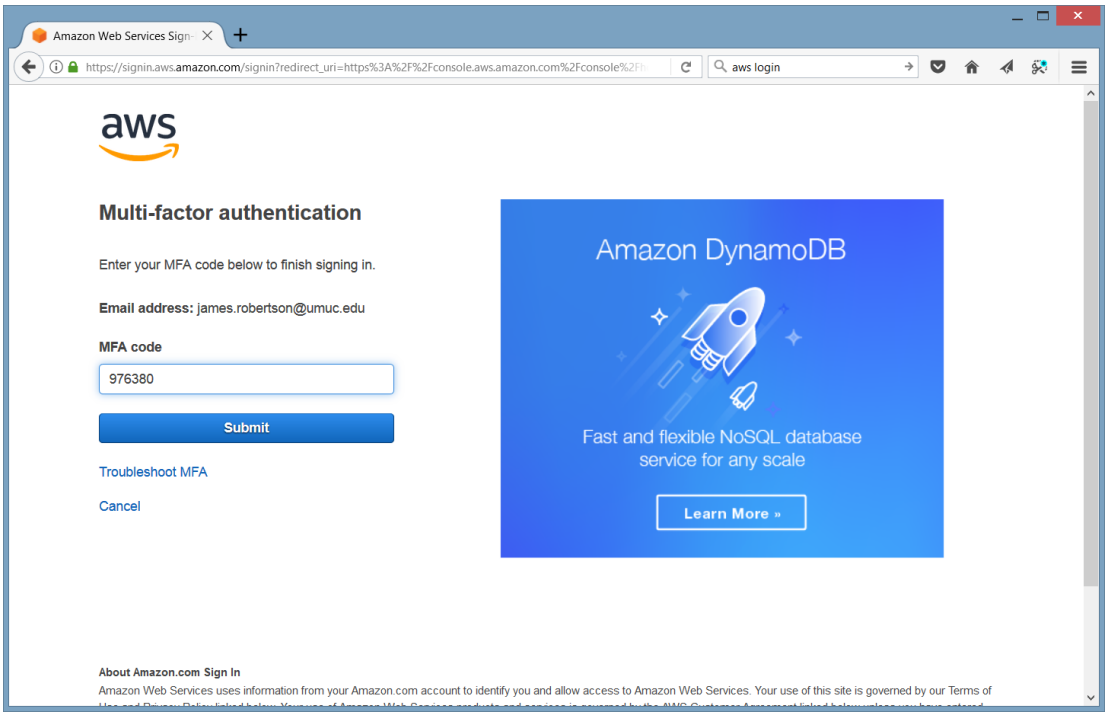

Figure 21 Entering your 6-digit authentication code

5. Next, you should create a group with Admin privileges, and then create a user to assign the group privileges. This is the user you will be using to login to the AWS console for the rest of this semester.

As shown in figure 22, to create a new group, select “Groups” from the IAM dashboard and then select “Create New Group”.

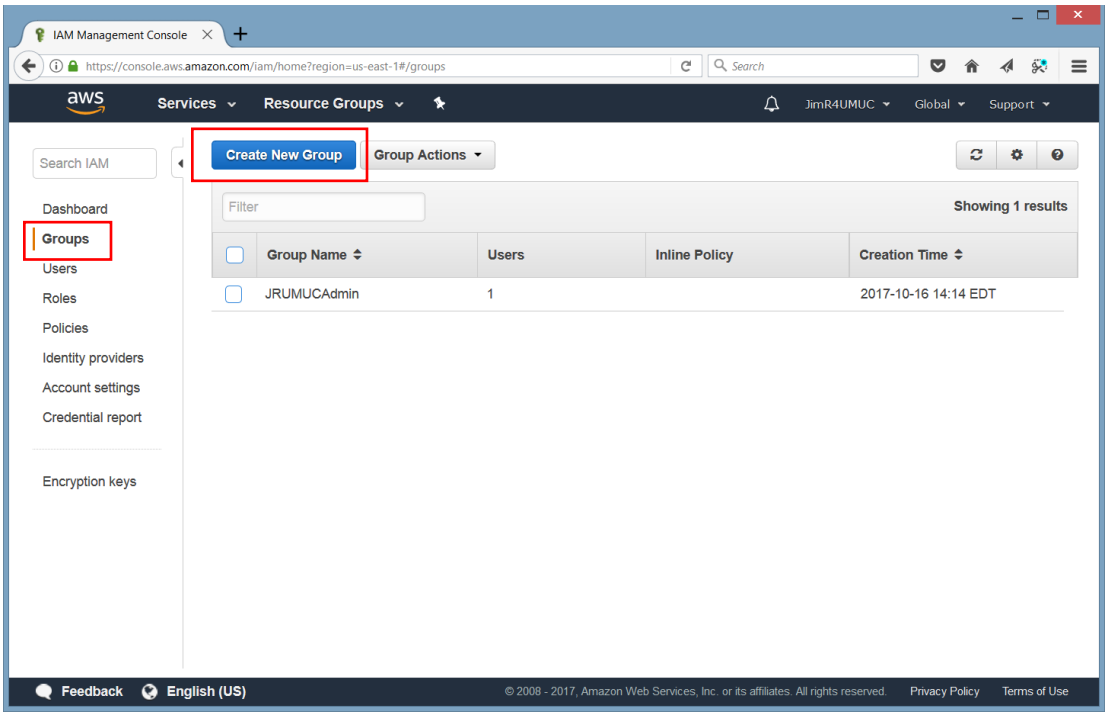

Figure 22 Creating a Group

As shown in figure 23, namel the group anything that makes sense (e.g. myAdmins) and then select “Next Step”.

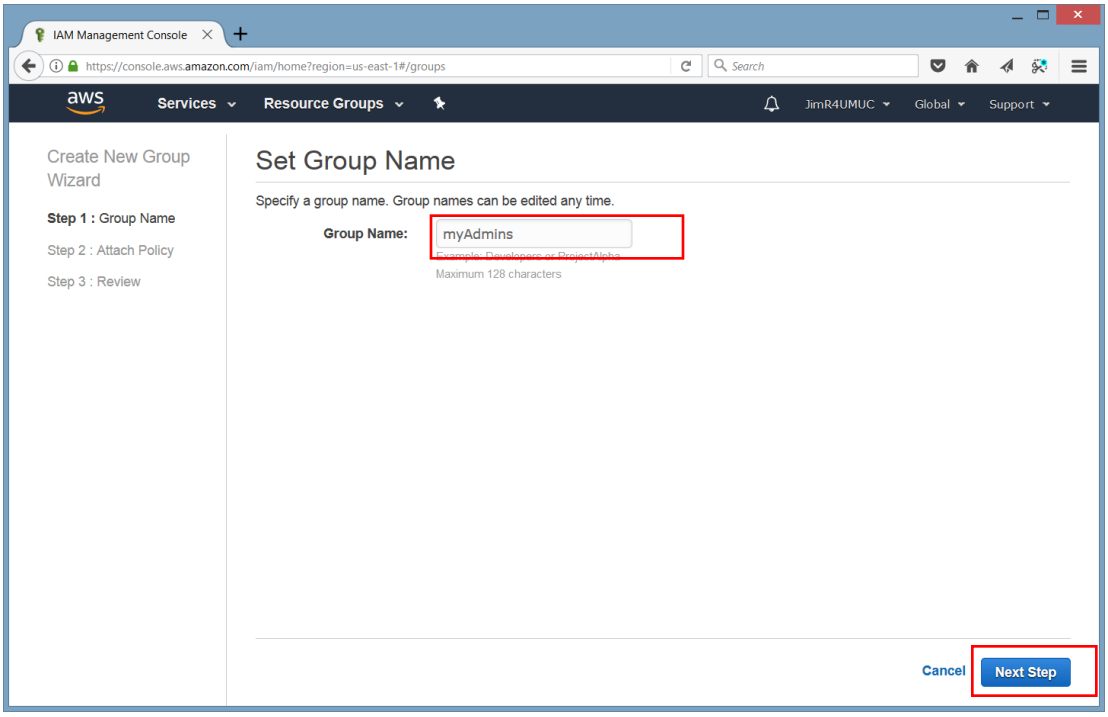

Figure 23 Naming the new group

Select the AdministratorAccess policy from the long list of available policy names and select “Next Step” as shown in figure 24.

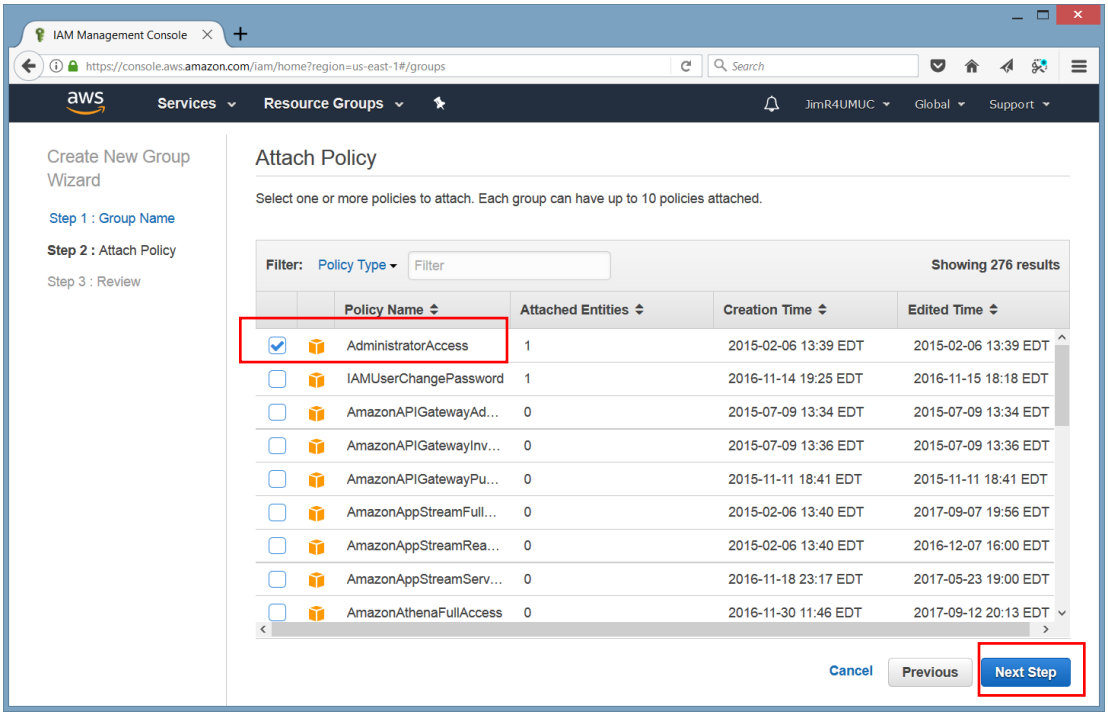

Figure 24 Select Administrator Access

As shown in figure 25, review the policy assigned and then select “Create Group”.

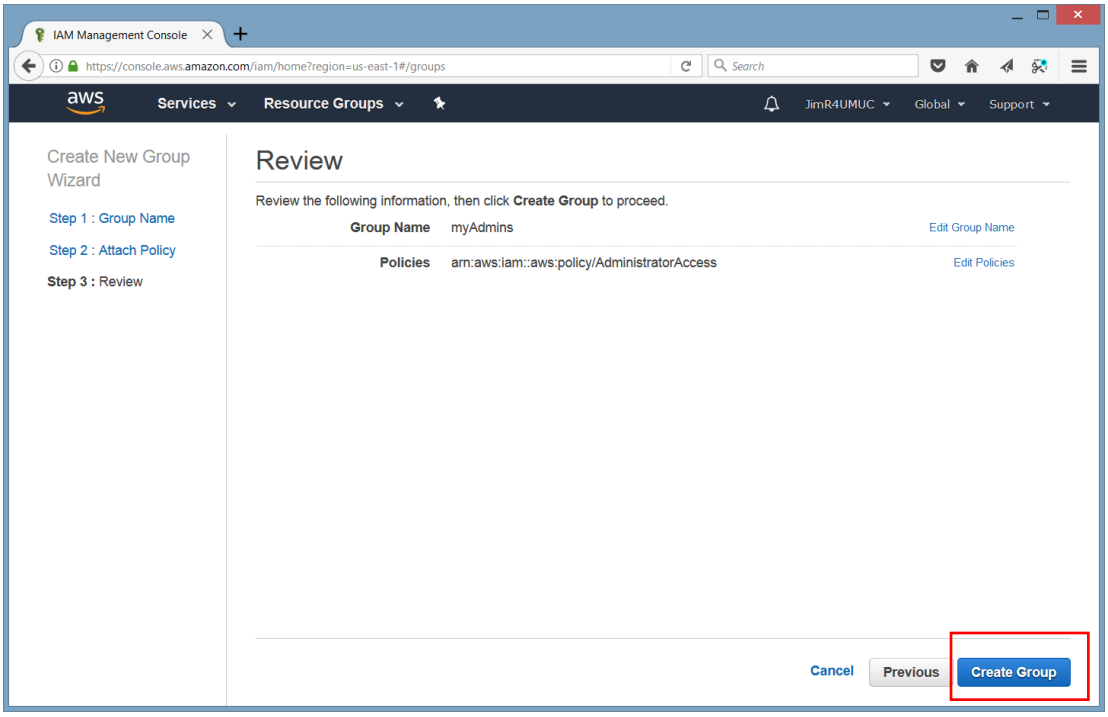

Figure 25 Creating the Group

As shown in figure 26, notice the myAdmins group has been added to the groups and currently, there are 0 users associated with it. We are about to add a user and then associated that user to the newly created group.

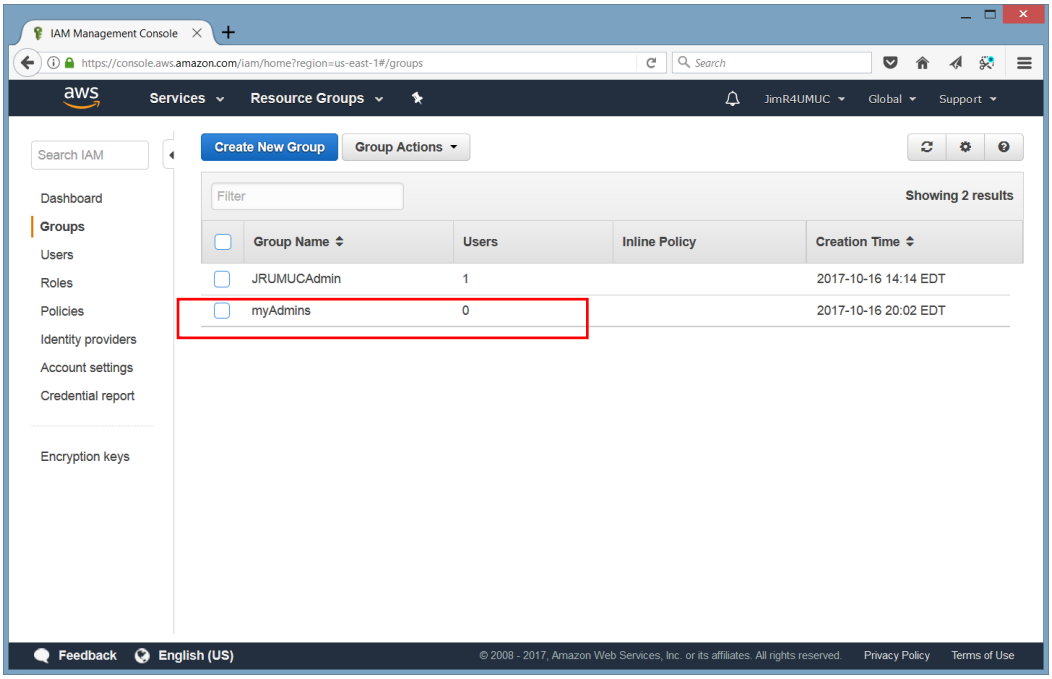

Figure 26 The Admin Group was created

To create a user for your myAdmins role, go the IAM dashboard and select “Users” as shown in figure 27.

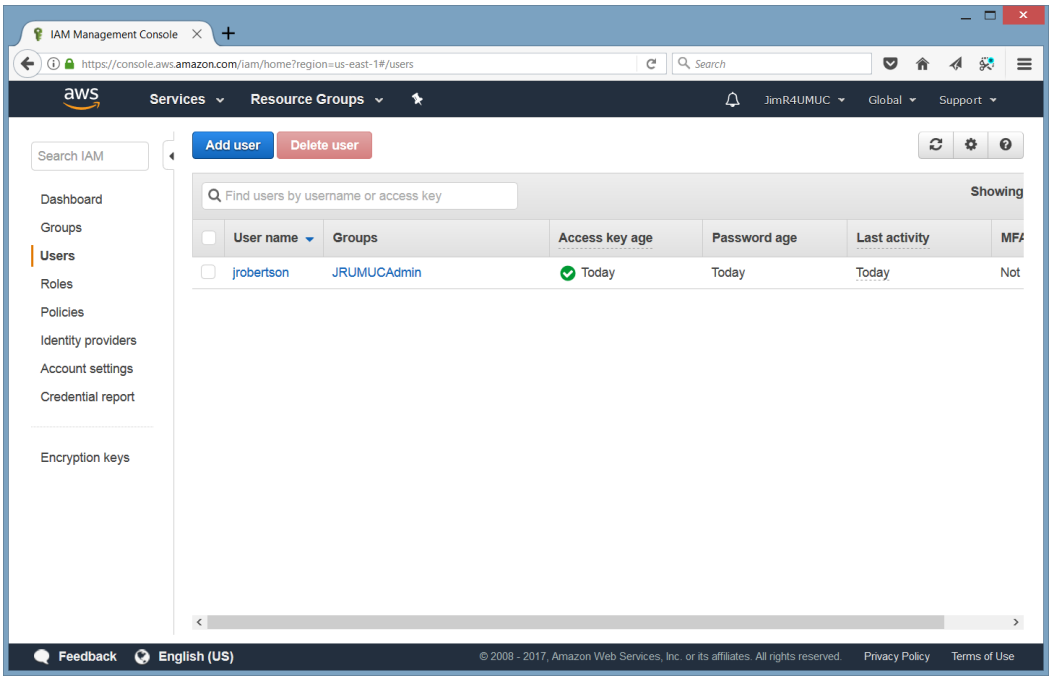

Figure 27 Creating a new user

Select Add User and enter the appropriate information for the user. Typically an admin user should have both programmatic and console access. Allow the system to automatically generate a password and require the password to be reset on their first login. (See figure 28).

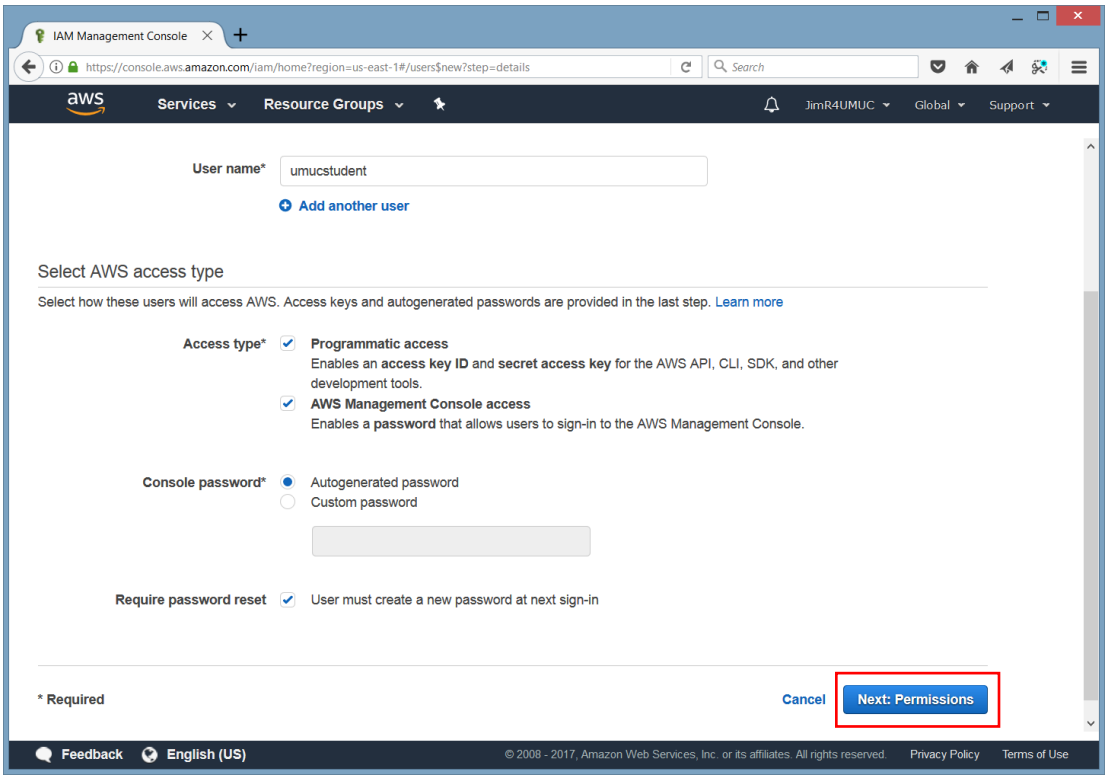

Figure 28 Creating the User Password

Click “Next:Permissions” to assign the group permissions created in the previous step. As shown in figure 29, click on the myAdmins group to automatically assign any permissions aligned with the myAdmins group to the new user.

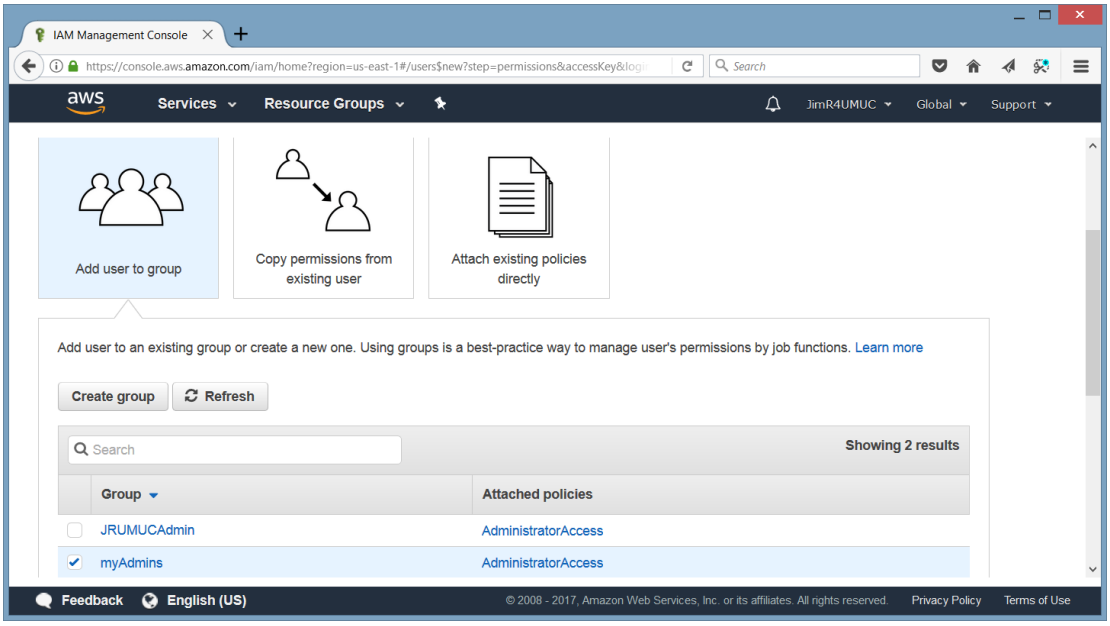

Figure 29 Assigning Permissions

As shown in figure 30, click Next to review and finally “Create User” to create the user with the Admin permissions. This is a non-root admin user that will be used for most of the work in this class.

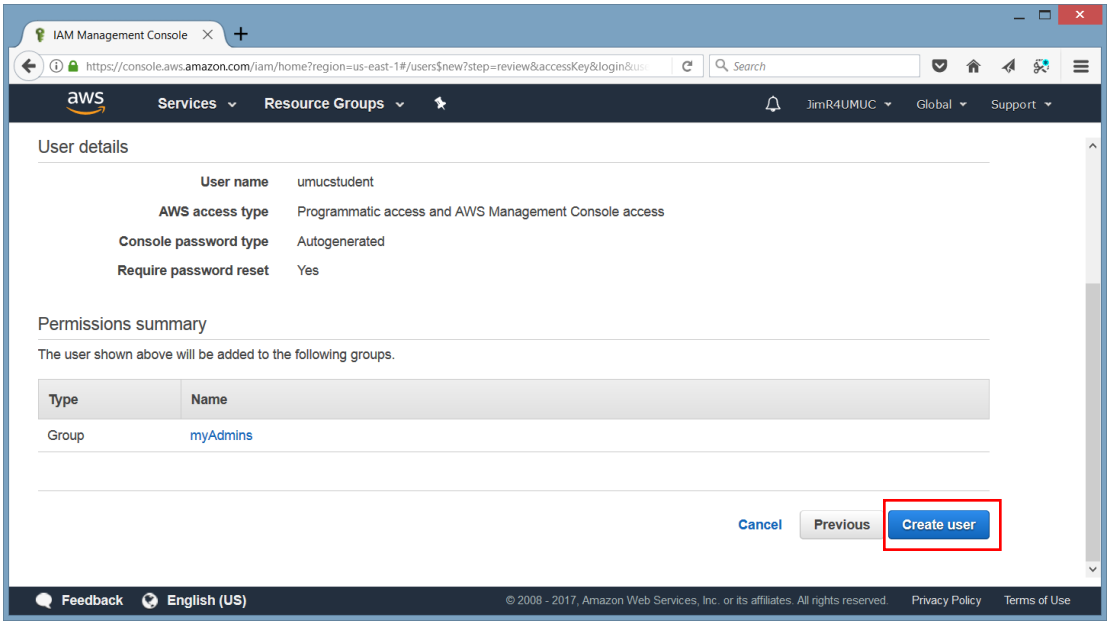

Figure 30 Finally - Create the User

As shown in figure 31, the system will generate some important credentials. You can download the .csv file, but be sure to store and protect it properly. You should also click on the “show” password to reveal a randomly generated password. You will need this to test your non-root, admin user login.

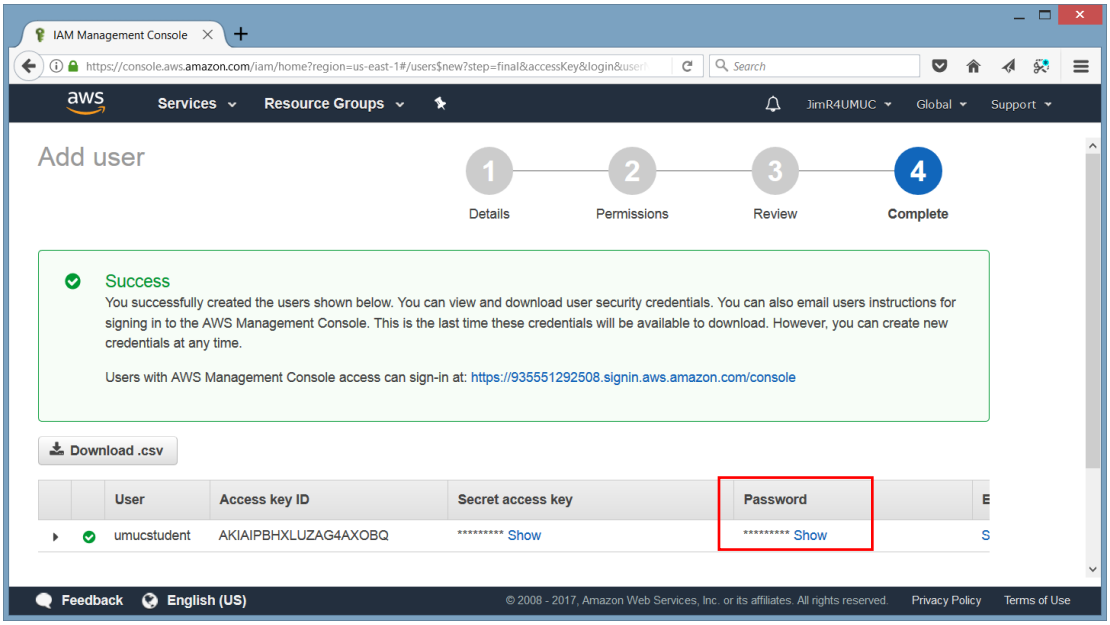

Figure 31 User Credentials Download

There is an email credentials option but currently, that feature does not seem to be working properly. Therefore, using the download and recording the password credentials is a better option.

As shown in figure 32, the .csv file will provide the initial password, Access and Secret Keys as well as the login URL information:

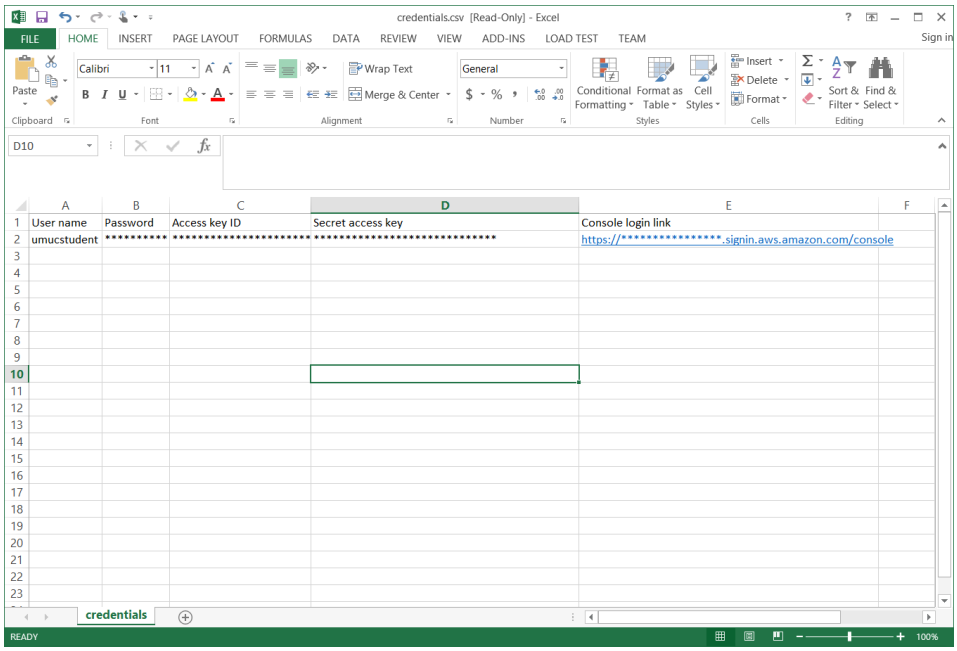

Figure 32 CSV login credentials

6. Finally, set your Password policy by clicking on the Account Settings in IAM.

As shown in figure 33, there are many options available for setting your password policy. Typically, the password should be at least 8 characters in length and have lower, upper, number and special characters. You can also set the password expiration dates and other options as needed.

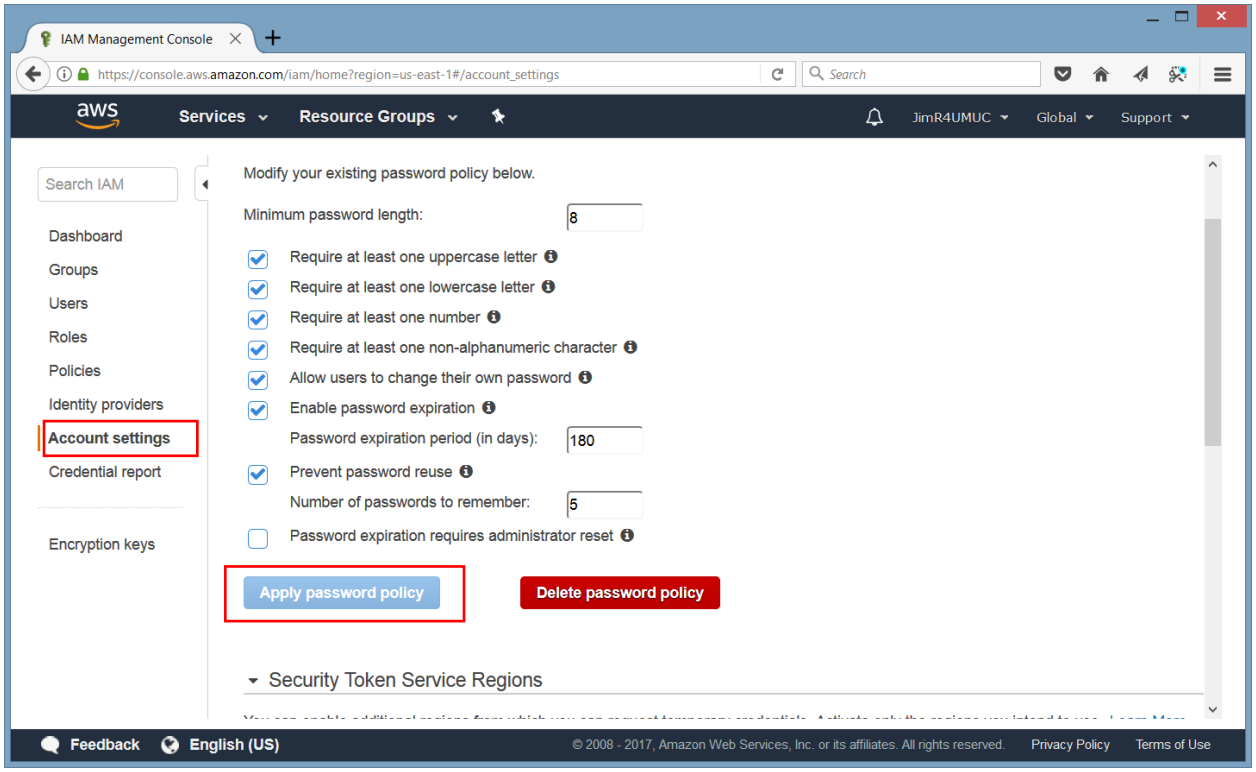

Figure 33 Setting the password policy

After completing these steps, all of the initial security best practice related to root access will be checked off as shown in figure 34.

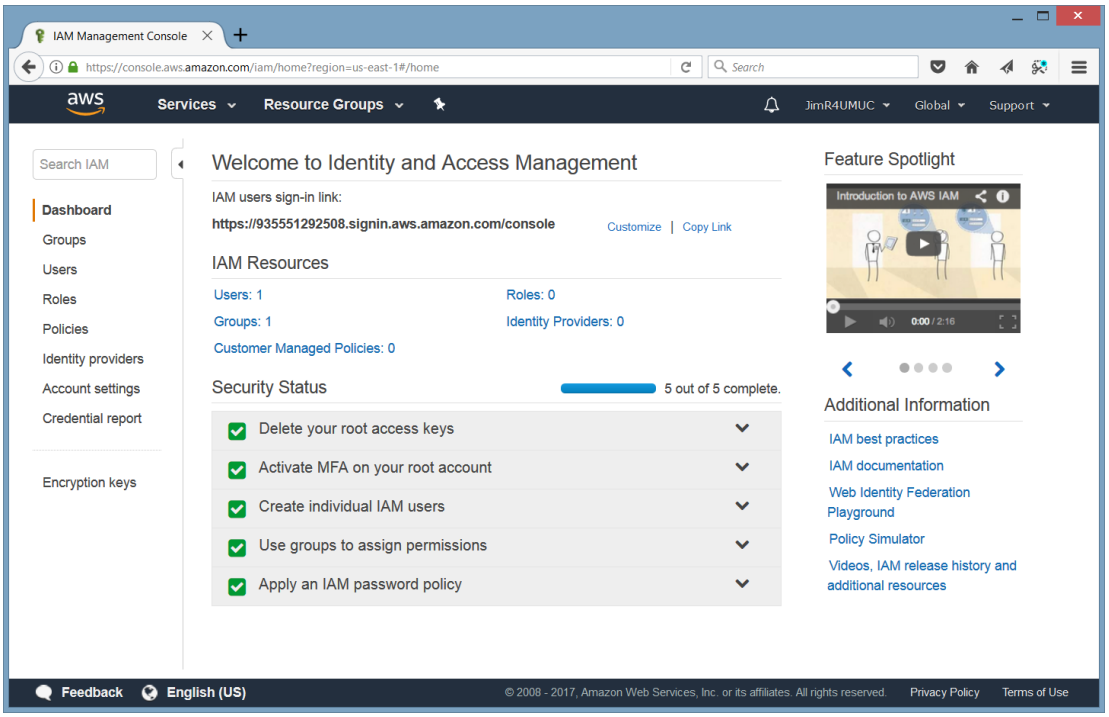

Figure 34 Securing your AWS Account

As mentioned before, for most future sessions you should login to the AWS console using your non-root, admin privileged account you just created.

The sign-in URL is provided in your .csv credentials folder.

It is typically similar to this:

https://931111111111.signin.aws.amazon.com/console

Where the numeric part of the URL is your unique 12-digit AWS account.

To test your login, go to URL and enter your newly created username and the password you were provided in the .csv file. Click "Sign-in" to continue. (See figure 35).

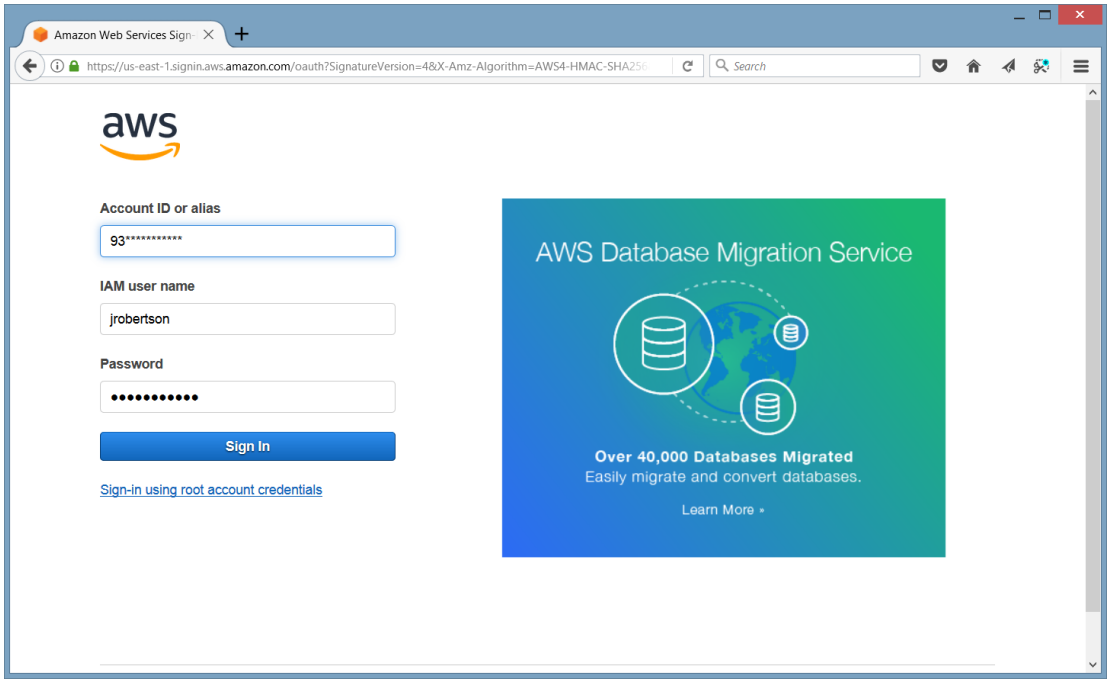

Figure 35 Signing in with your non-root, admin account

Note: you should be prompted for a password change if you correctly configured your account. Be sure to record your new password.

There are several screen captures and documentation required to for you to earn points for this lab as described below.

Lab 0 Submission Requirements and Grading Rubric:

The submission should include 3 components in a word or PDF document including:

1. Your 12-digit unique AWS ID. Note: It is expected that this account will be used throughout all SDEV classes at UMUC that use AWS services.
2. A copy of the congratulations email from AWS Education showing you are now an AWS Educate member that includes the $100 AWS grant. (**Be sure to redact the AWS Credit Code before submitting.)**

3. Screen capture demonstrating all 5 security best practices related to your root account were successfully accomplished. (See figure 34. Be sure your 12-digit AWS number is clearly visible in this screen capture.)

Any submissions that do not represent work originating from the student will be submitted to the Dean's office and evaluated for possible academic integrity violations and sanctions.