# Enabling Multi-Factor Authentication on Your AWS Account

### Introduction

AWS allows you to improve IAM security by enabling multi-factor authentication (MFA). Enabling MFA requires an additional code to be entered when accessing AWS services. Two forms are supported:

* **Security token-based**: A security token is sent to a physical or virtual MFA device
* **SMS text message-based**: A code is sent to an SMS-compatible mobile device

Only security token-based MFA is allowed for the root account. This Lab Step will walk through setting up security token-based MFA using a virtual device.

Note: You will need to install an MFA application on your mobile device to complete this Lab Step. If you prefer not to install an MFA application, you can skip the Lab Step or only read the instructions

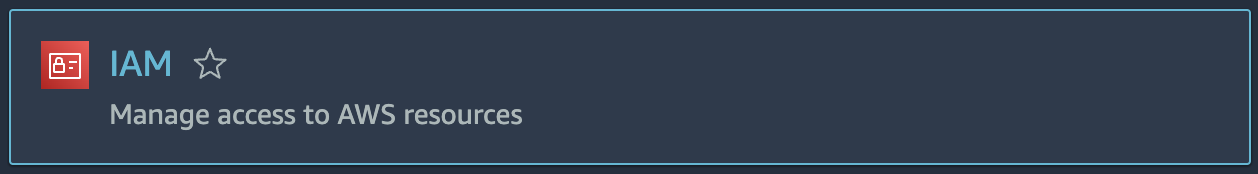
### 

### Instructions

1. Install a compatible virtual MFA application on your mobile device.

Amazon provides a list of applications for a variety of device types on their [multi-factor authentication page](https://aws.amazon.com/iam/details/mfa/) in the **Virtual MFA Applications** section. The page provides links to installation instructions.

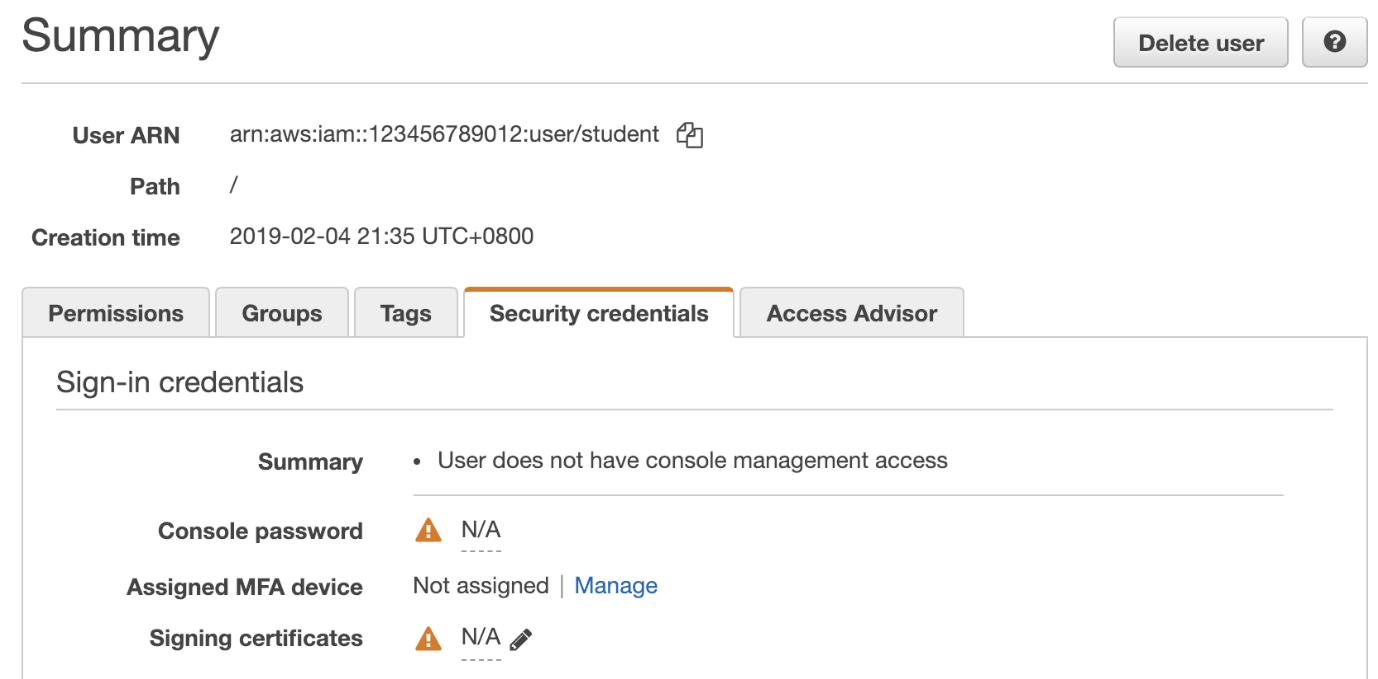
2. In the Management Console, in the search bar at the top, enter IAM, and click the **IAM** result under **Services**:



alt Warning! You will see error messages on this page and following IAM pages. This is normal. You only have the permissions required to complete the Lab.

3. Click **Users** in the left navigation panel.

4. Click on the **student**user and select the **Security credentials** tab:

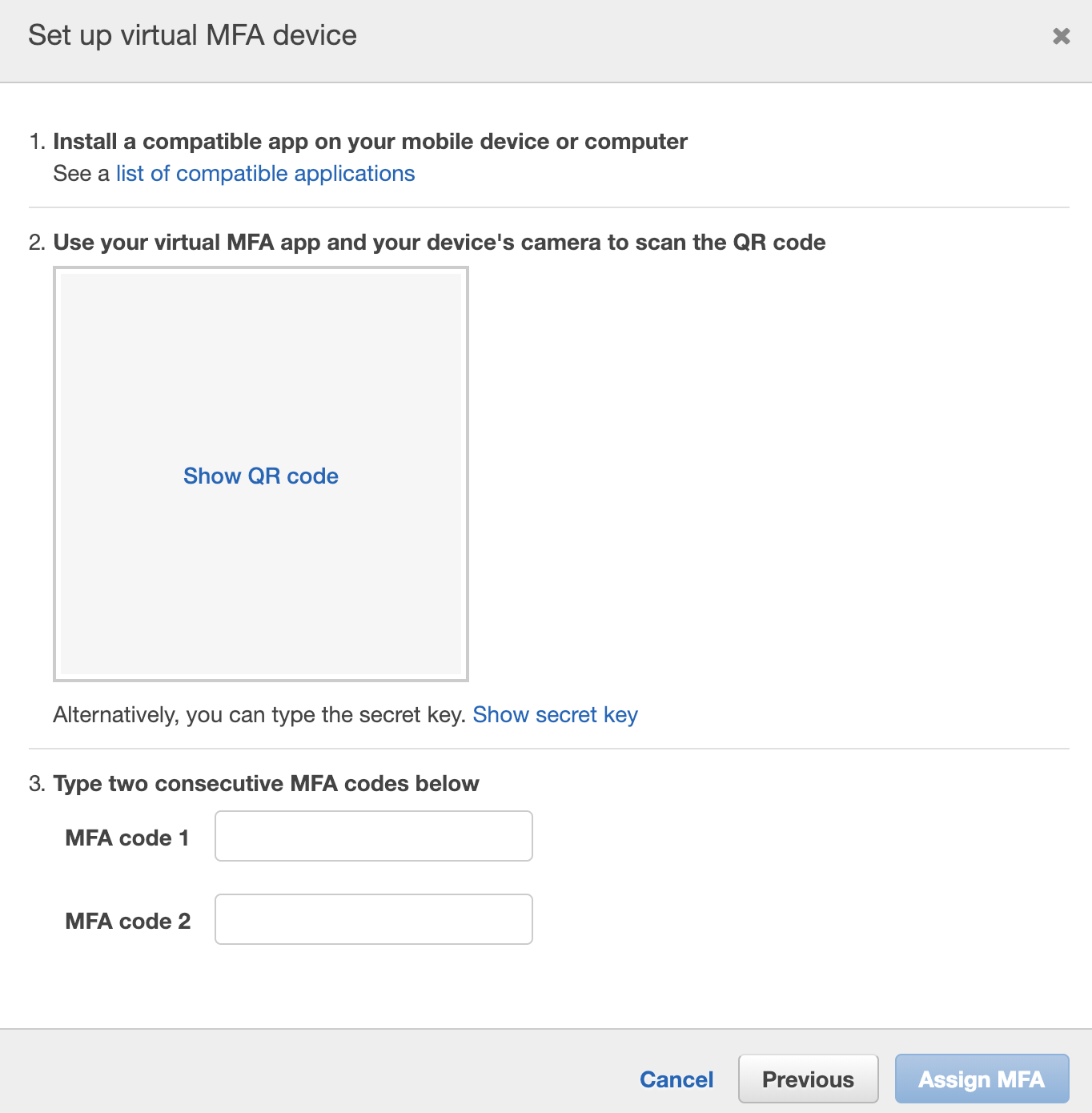


5. Click on **Manage** to the right of **Assigned MFA device**.

6. In the **Manage MFA Device** dialog, select **Virtual MFA device** and click **Continue**.

7. Click **Next Step**when prompted to be sure you have an AWS-compatible MFA application installed.

8. Click **Show QR code** to reveal the QR code:



Scan the QR code with your virtual MFA application if it is supported. Otherwise, click **Show secret key**for manual configuration.

8. Follow the instructions in your virtual MFA application to configure the application.

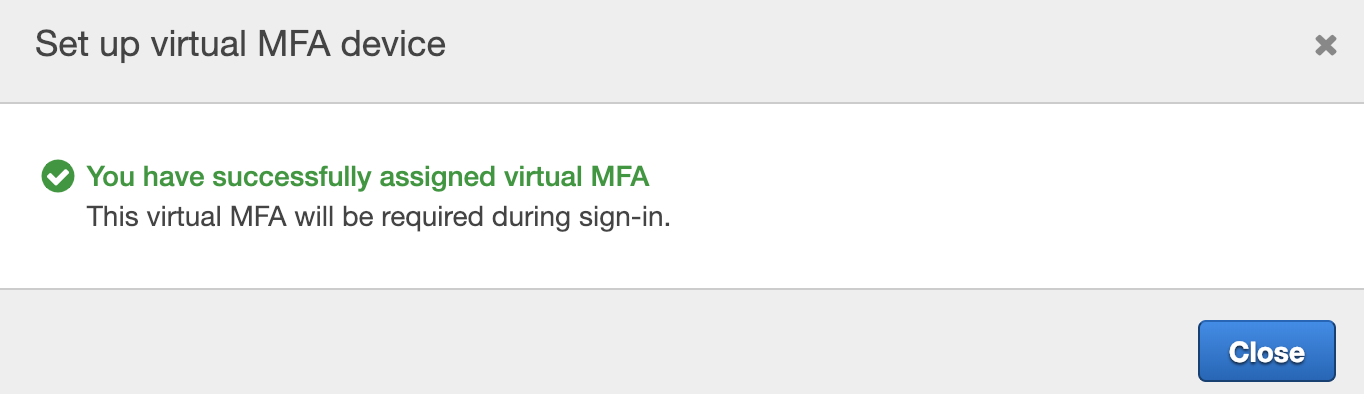
9. Enter the code the application gives you in **MFA code 1** of the **Set up virtual MFA device**dialog and wait until you have a second code in your virtual MFA application.

10. Enter the second code from the application into **MFA code 2**.

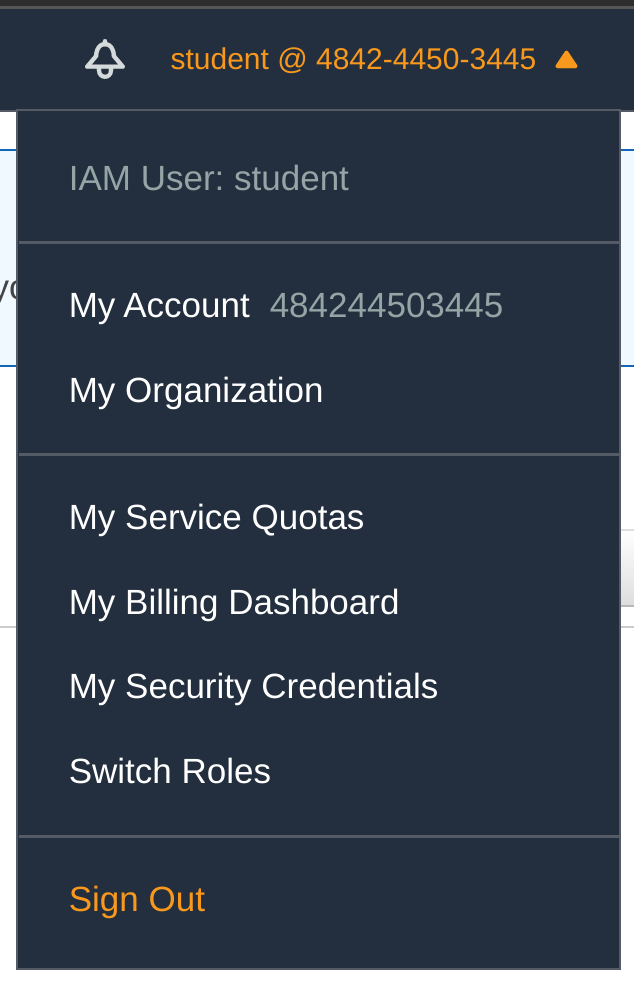
11. Click **Assign MFA**.

The virtual MFA device is now ready for use with AWS.

12. Click **Close** to the confirmation dialog box:



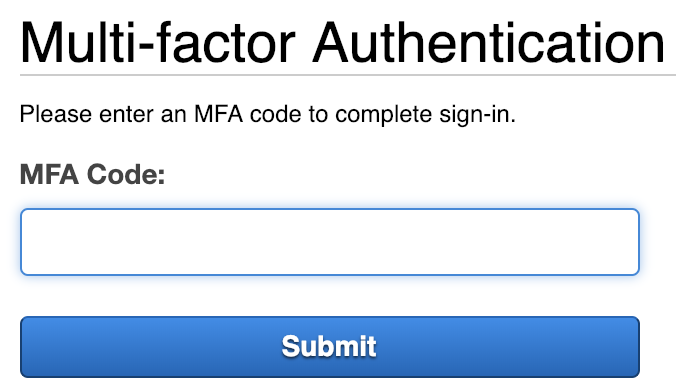
13. Try out the MFA by clicking on **student** on the right side of the top navigation bar and selecting **Sign Out**:



14. Click **Log back in** on the AWS Management Console homepage.

15. Enter the **User Name**and **Password** in the **Your lab data**section of this Lab and click **Sign In**.

16. On your virtual MFA device, generate a new code in the virtual MFA application and enter it into the **MFA Code** and click **Submit**:



### Summary

In this Lab Step, you enabled MFA on your account using security token-based MFA. You used an MFA application on your virtual MFA device. You also tested the MFA by signing into the AWS Management Console using an MFA code.