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.

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

![AWS Account Creation Screen](image)

**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."  

![My Account Menu](image)  

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

### Alternate Contacts

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

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/](https://aws.amazon.com/organizations/)  

### IAM User and Role Access to Billing Information

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.

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 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."

   ![Manage Security Credentials](image)
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:

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.

<table>
<thead>
<tr>
<th>Device</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Google Authenticator; Authy 2-Factor Authentication</td>
</tr>
<tr>
<td>iPhone</td>
<td>Google Authenticator; Authy 2-Factor Authentication</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>Authenticator</td>
</tr>
</tbody>
</table>
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.
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.

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

![IAM users sign-in link](image)

6. **Sign out of your AWS account.**

![Sign Out](image)

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

![Sign In](image)
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.
Fixing the IAM Dashboard Warnings

Add a Group

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

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

3. Click the "Create New Group" button.
4. Enter group name "Sec545admin" and click "Next Step".

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

6. Review and click "Create Group."
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.

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

   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