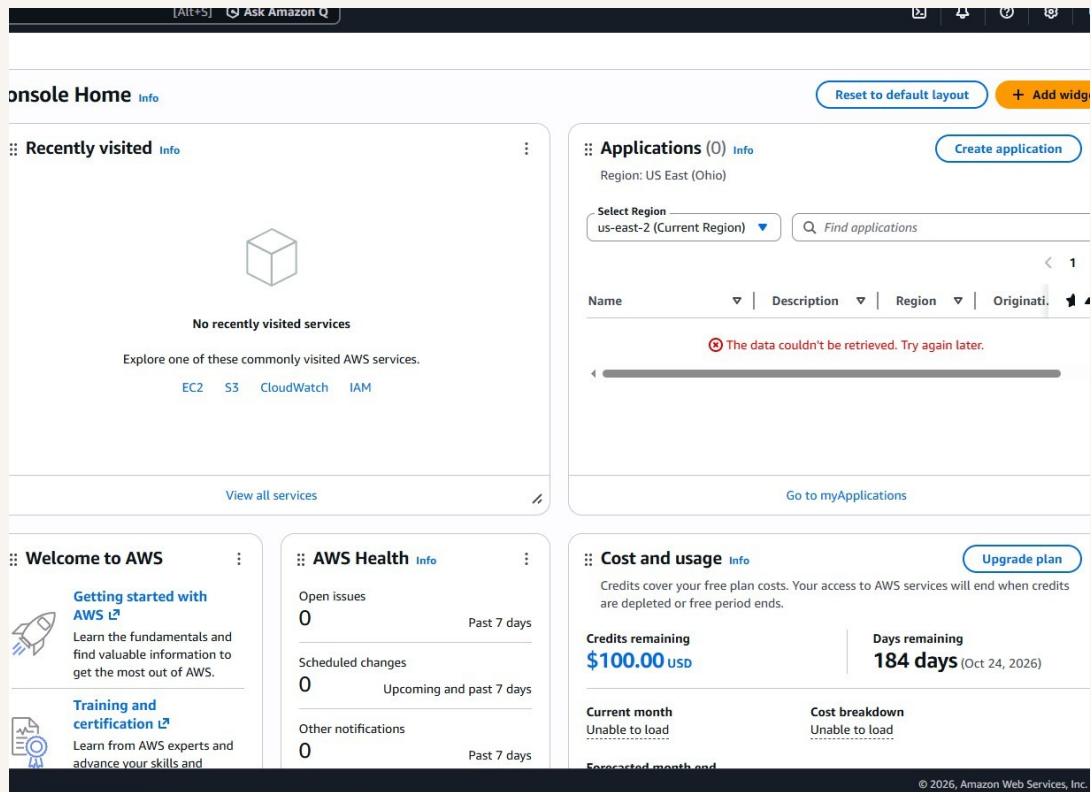


Set Up an AWS Account

Melvin green



Introducing Today's Project!

Create and fully activate the AWS account. Complete identity verification, add a payment method, and confirm you can sign in as the root user. Store root credentials securely (preferably in a password manager). Set up billing alerts. Enable Billing Alerts in the AWS billing preferences. Create an Amazon CloudWatch billing alarm. Configure email notifications through Amazon Simple Notification Service (SNS)

Consider creating an AWS Budgets budget as an extra safeguard Add Multifactor Authentication, and enable MFA on the root account immediately. Prefer an authenticator app or hardware security key over SMS Save backup/recovery codes securely. Test sign-in once MFA is enabled

Key tools and concepts

Through this project, I learned the foundational steps for securely setting up an Amazon Web Services account. This included creating root user credentials, adding a payment method, understanding the AWS Free Tier options, setting billing alerts, completing identity verification, choosing a support plan, and enabling Multi-Factor Authentication (MFA) to strengthen account security. Key Concepts Root User Security – The root account has full administrative access, so it should be protected with a strong password and MFA. Billing Awareness – Setting billing alerts helps monitor usage and avoid unexpected charges. AWS Free Tier – Understanding Free Tier limits is important for using AWS services without unnecessary costs. Account Verification – Identity verification and support plan selection are required steps to fully activate an AWS account.

Challenges and wins

This project took me approximately 15 minutes. The most challenging part was familiarizing myself with the AWS dashboard.

Creating My AWS Account

I created an account in the Amazon Web Services portal using my email address and selected an account name/username. After submitting my information, I verified my email address using the verification code sent to my inbox. Once verification was complete, I created a secure root account password to finish the initial account setup.

Understanding the root user

I learned that the root user in Amazon Web Services has full administrative access to the account, including billing, security settings, and access to all AWS services. Because the root user has complete control over the account, creating a strong, unique password is essential to help prevent unauthorized access by unwanted users.

Setting Up Billing and Payment

In this step, I selected the free account plan offered by Amazon Web Services. After choosing the plan, I entered my contact information and added a payment method to complete the account setup process. This information is required for account verification and billing, even when using free-tier services.

Why AWS requires a payment method

I learned that AWS requires a payment method because. AWS places a temporary \$1 authorization to verify my card.

Completing Account Activation

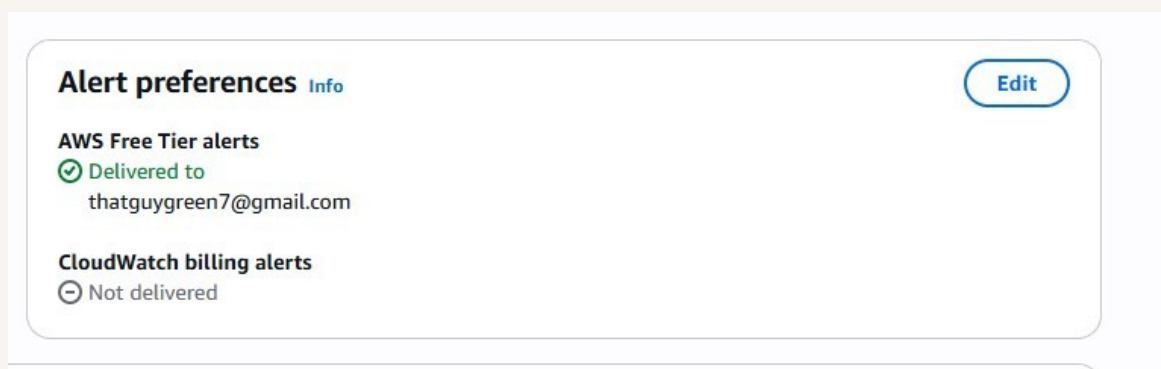
In this step, I confirmed my identity as part of the account verification process. This may include verifying a phone number or completing other security checks. After my identity was confirmed, I selected a support plan to finish setting up the account.

Identity verification and support plan

I verified my identity by using SMS messages via phone. The Basic support plan includes 24/7 self-service to AWS resources and access to a personal Health Dashboard & trusted advisors.

Enabling Free Tier Alerts

In this step, I'm going to navigate to billing presences and enable free tier usage alerts.



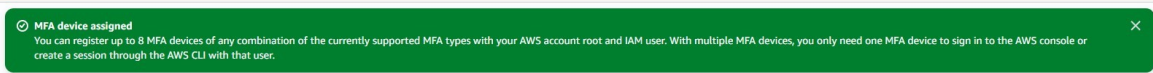
Why usage alerts matter

I set up usage alerts to protect my account from unexpected charges.

Securing the Account with MFA

To improve account security in Amazon Web Services, I enabled Multi-Factor Authentication (MFA) for the root account. In the Security recommendations section, I clicked Add MFA and entered a name for the MFA device, such as my phone or root-mfa. I then selected the Authenticator app as the MFA method and clicked Next. After clicking Show QR code, I scanned the QR code using my authenticator application. I entered the first generated verification code in the MFA code 1 field, waited for the code to refresh, and entered the next

generated code in the MFA code 2 field. After submitting both codes, I clicked Add MFA to complete the setup. Why MFA is Important: Multi-Factor Authentication adds an extra layer of protection by requiring two or more forms of verification to confirm identity. This typically combines something you know, such as a password, with something you have, such as a phone or authenticator app, and in some cases, something you are, such as biometric verification. Enabling MFA



MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.