Service Brief

How to Protect Your AWS Root User Account

OVERVIEW

AWS is the current leader in the cloud computing space, and with this leadership position comes great risk. When launching an AWS account, you first create the AWS Root User Account. The AWS Root User Account is the most powerful account in your AWS environment. This account has complete control over all your AWS resources, billing details, and account contact information. If your root user account is compromised, it can wreak havoc on your organization. For example, a bad actor could use it to cause disruptions to your business, run up large bills on your AWS account, and could even launch a cyber-attack.

For traditional system admins, the AWS Root User Account is the equivalent of having the root user account on a Linux /Unix server or being an Enterprise Admin on a Microsoft Windows Domain.

Securing your AWS Root User Account is critical to preventing a cyber incident and protecting your data from unwanted exposure. The Seven Best Practices to Securing Your Account

Here are the top seven best practices to follow to ensure your AWS Root User Account remains secure.

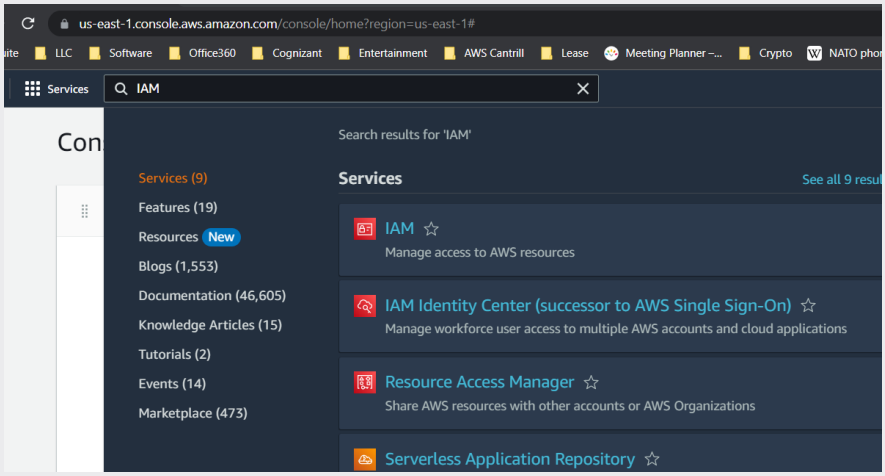
1. **Enable multi-factor authentication (MFA):** MFA adds an extra layer of security to your Root User account, requiring a code from a physical device and the password to log in.
2. **Use a strong and complex password:** The Root User should have a password that is long, complex, and includes a combination of letters, numbers, and special characters.
3. **Limit access:** Restrict access to the Root User Account to only those who absolutely need it.
    - You should not use your root user account for daily activities.
    - You should grant non-root user accounts within IAM to access features like billing rather than using your root user account.
4. **Enable AWS CloudTrail:** AWS CloudTrail provides visibility into user activity and resource changes across your AWS accounts. Enable it to track all activity in your AWS account, including root account activity.
5. **Regularly monitor and audit activity:** Review the activity logs generated by AWS CloudTrail and other logging tools to detect and respond to suspicious or unauthorized activity.
6. **Access Key:** Do not create access keys for the AWS Root Account
7. **Use AWS Organizations to manage multiple accounts:** Use AWS Organizations to manage and automate creating and managing multiple AWS accounts centrally.

This can help to reduce the risk of accidental or unauthorized changes to your root account.

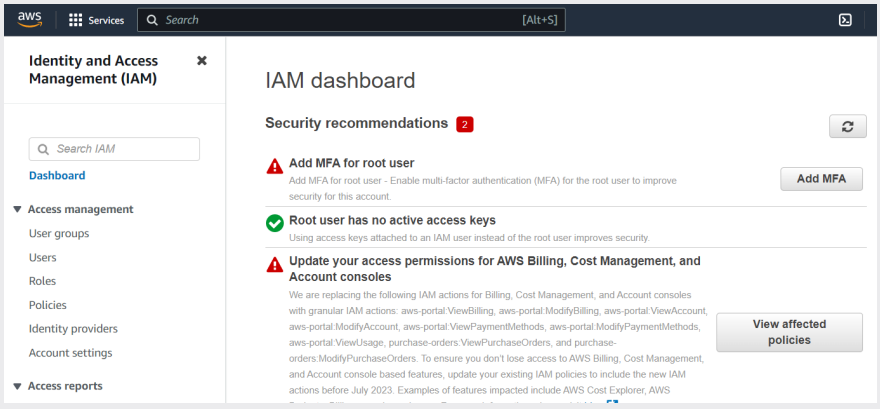
STEP-BY-STEP GUIDE TO SECURE SETUP

1) Use multi-factor authentication (MFA): MFA adds a layer of security to your root account. Configure MFA for all users with root account access to protect against unauthorized access.

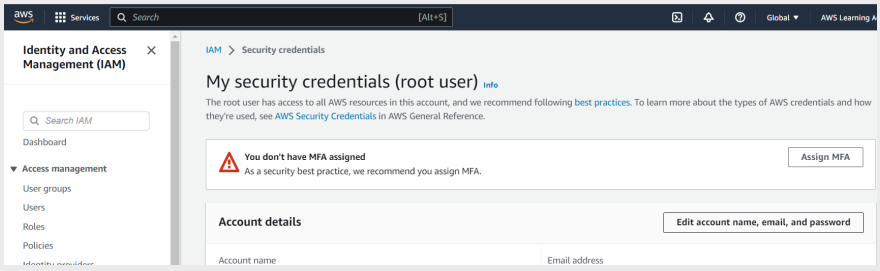
In the AWS console, open IAM



Click Add MFA



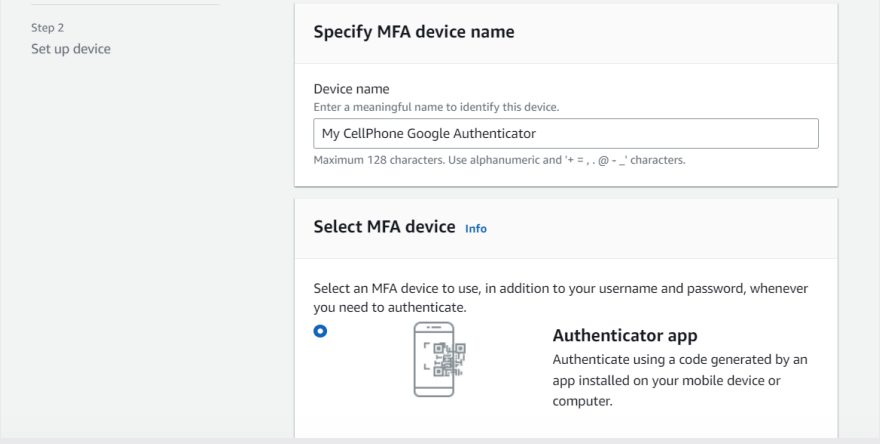
Click Assign MFA



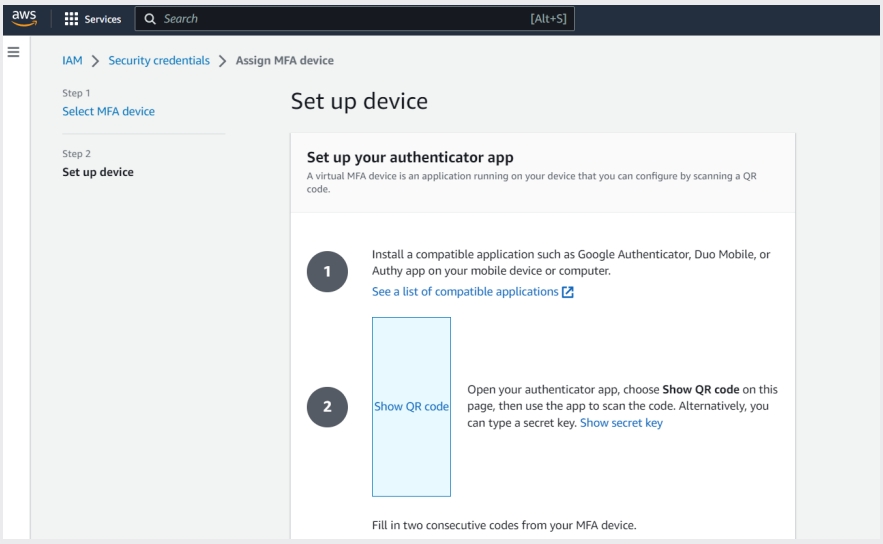
Enter a Name friendly name for the Authentication Device

For this example, we are using Google Authenticator on my cellphone.

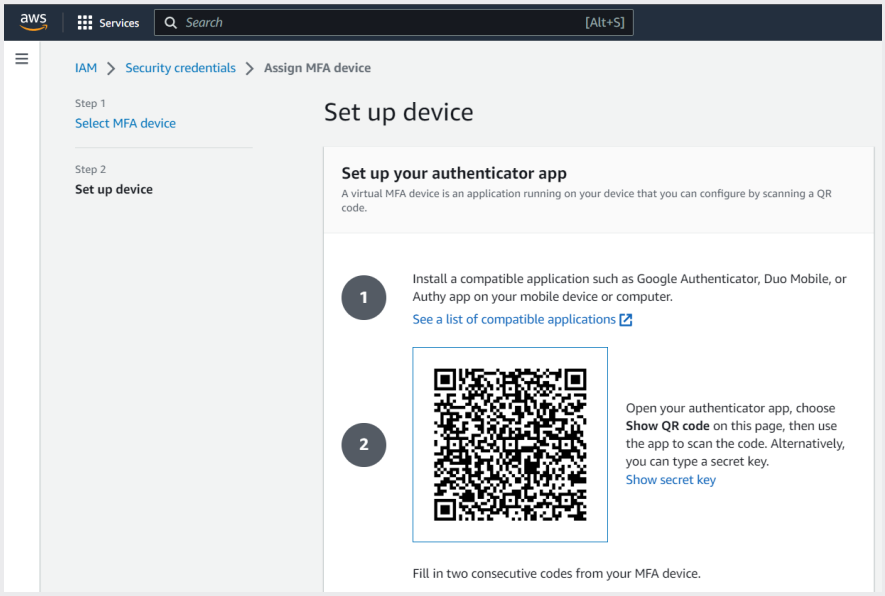
You can use any MFA software of your choosing.



For this example, we will scan the QR code on our phone.
This is the easiest way to set up MFA.

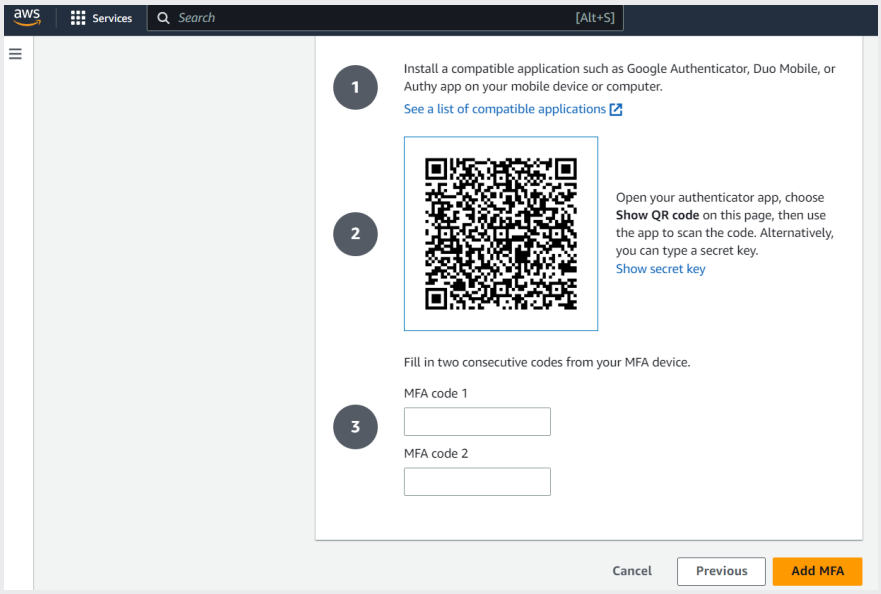


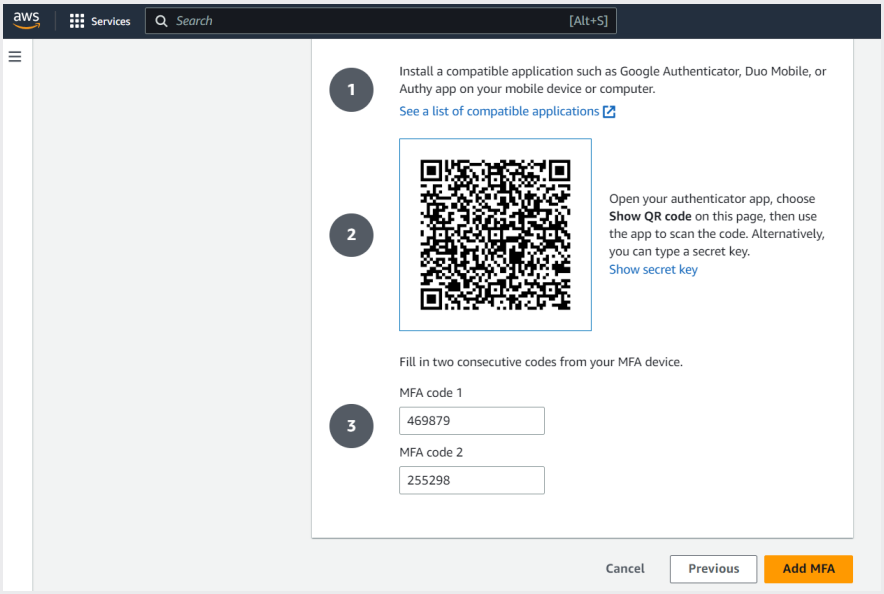
Click Show QR Code



Once the QR code has been scanned Enter the “MFA Code 1” and “MFA Code 1”

Click “Add MFA”.

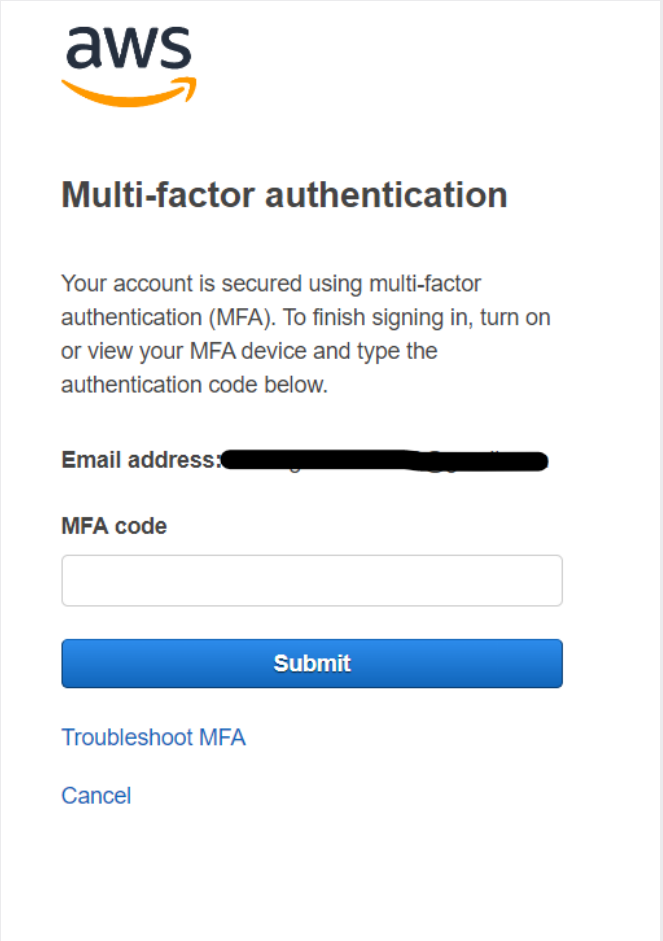




Now you have successfully secured your "Root" account with MFA.

Log out of the Account and give it a test.

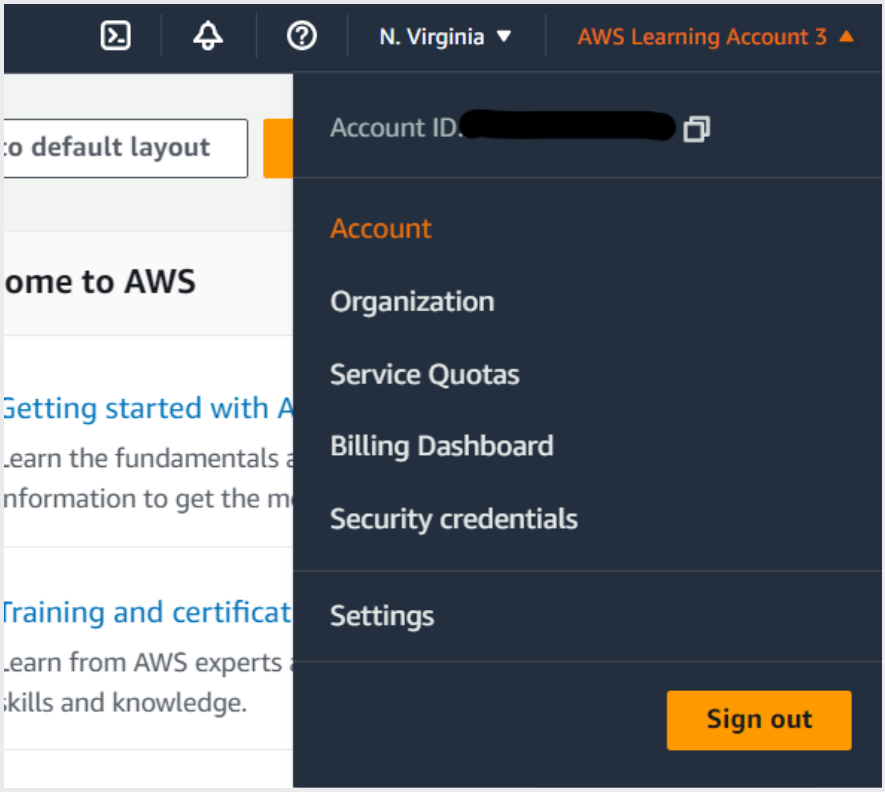
You should now be prompted to enter your "MFA code".



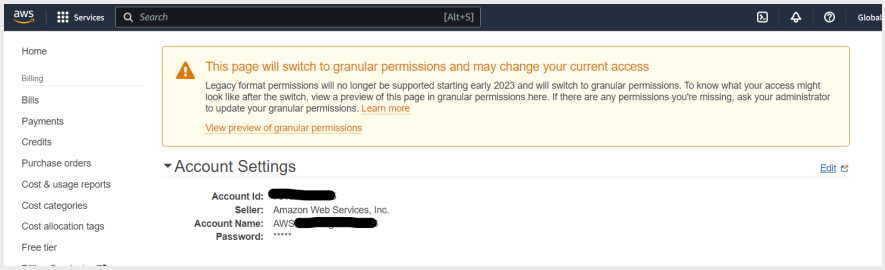
2) Use strong passwords: Ensure all users with root account access have strong passwords that meet AWS password requirements. Regularly update passwords to maintain security.

To change your root password

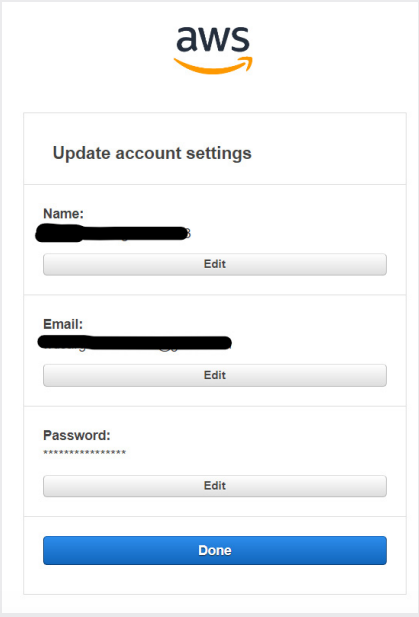
Click on the Account in the upper right-hand corner Account.



Click Edit



Click Edit Under Password



Enter a new Password:

Note the AWS Root password Policy.

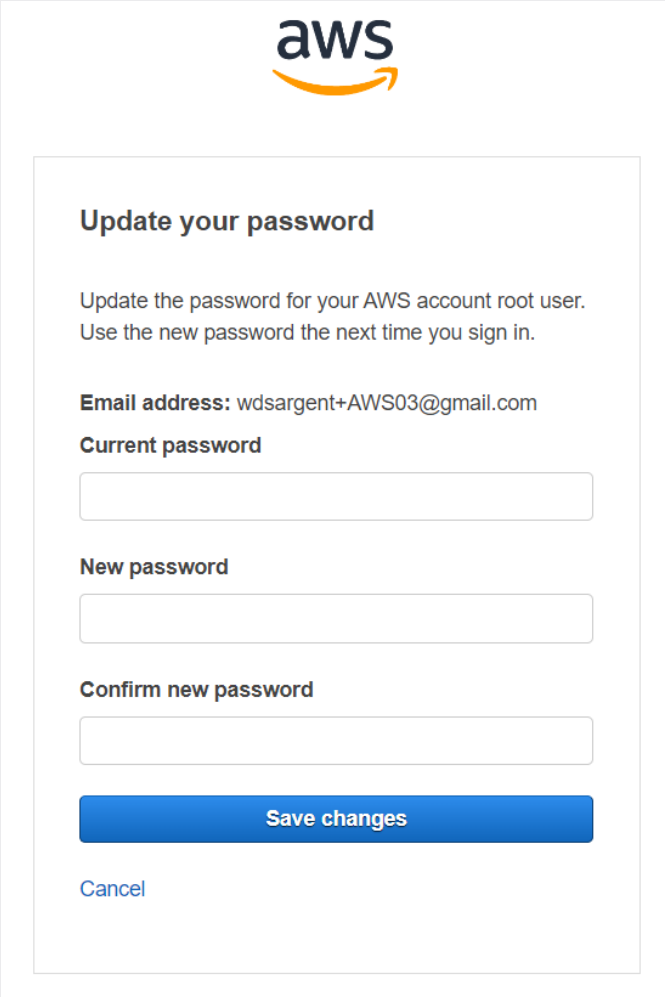
It must have a minimum of 8 characters and a maximum of 128 characters.

It must include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * () <> [] {} | _+-= symbols.

https://docs.aws.amazon.com/accounts/latest/reference/root-user-password.html

Enter the Old password then the New Password

Then click “Save Changes.”

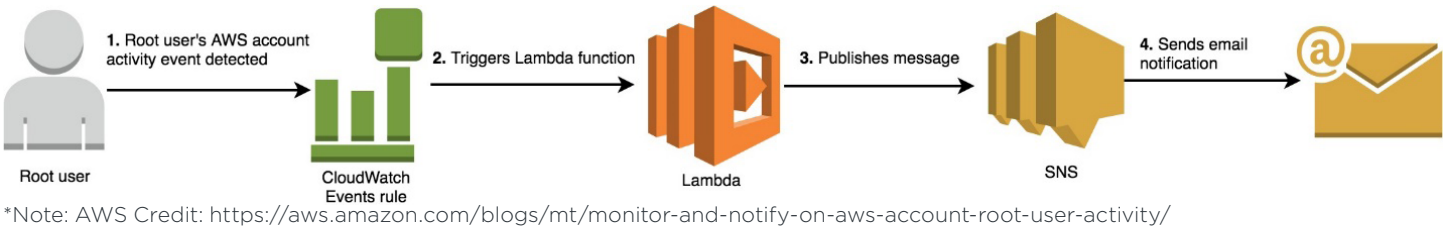


3) Limit root account access: Only grant root account access to the users who need it. Avoid using the root account for day-to-day activities and create individual IAM accounts with least privilege access instead!

4) Enable AWS CloudTrail: AWS CloudTrail provides visibility into user activity and resource changes across your AWS accounts. Enable it to track all activity in your AWS account, including root account activity.

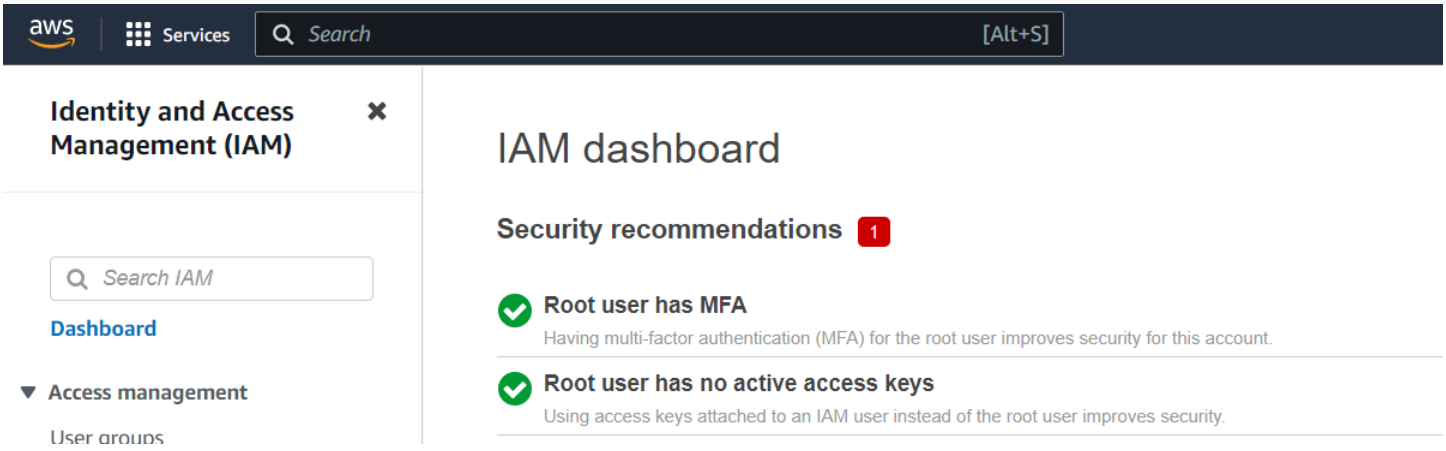
- Follow the Steps on this link to setup Cloud Trail audit for the Root Account
  - https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity/

5) Regularly monitor and audit activity: Review the activity logs generated by AWS CloudTrail and other logging tools to detect and respond to suspicious or unauthorized activity.



*Note: AWS Credit: https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity/

6) Access Keys: Don't create access keys for the root user.



7) Use AWS Organizations to manage multiple accounts: Use AWS Organizations to centrally manage and automate the creation and management of multiple AWS accounts. This can help to reduce the risk of accidental or unauthorized changes to your root account.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org.html

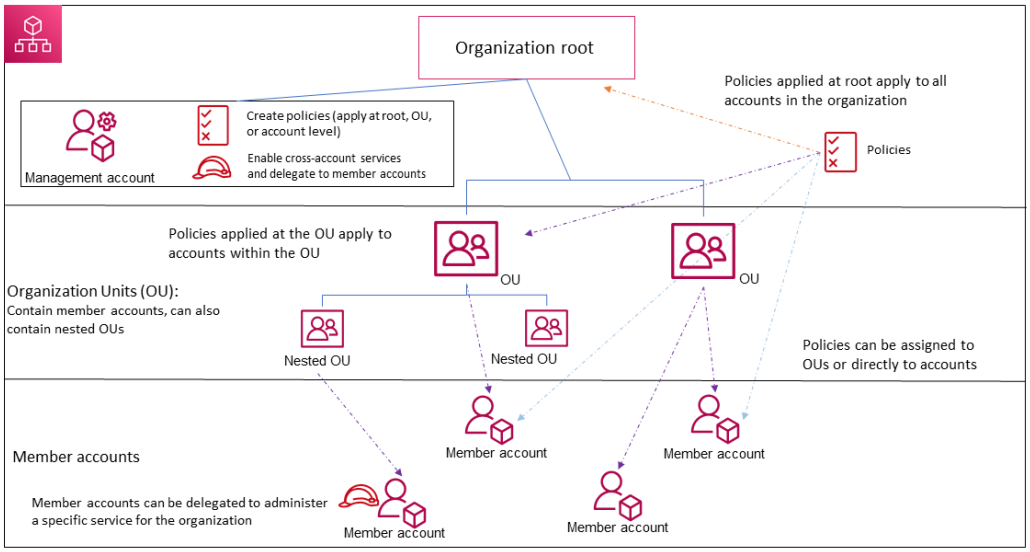


*Diagram: credits to AWS

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

SDG

Contact Us: solutions@sdgc.com

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com