

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.

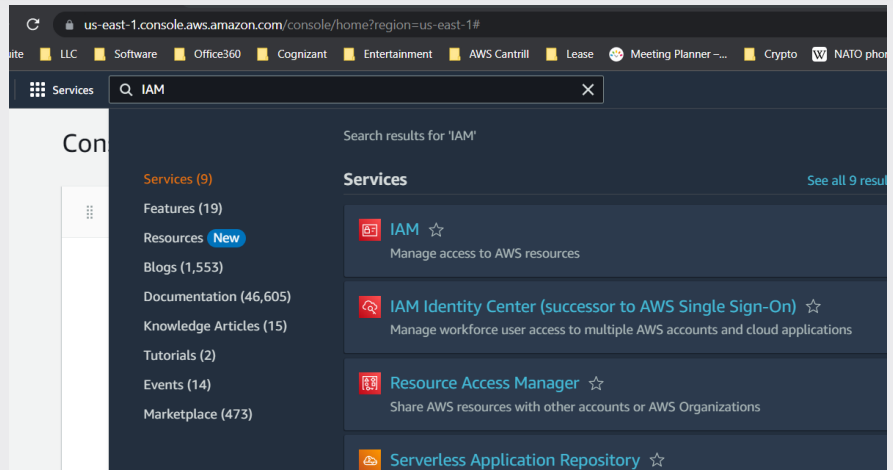
1. **Enable multi-factor authentication (MFA):** MFA adds an extra layer of security to your Root User account, requiring a code from a physical device and the password to log in.
2. **Use a strong and complex password:** The Root User should have a password that is long, complex, and includes a combination 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.

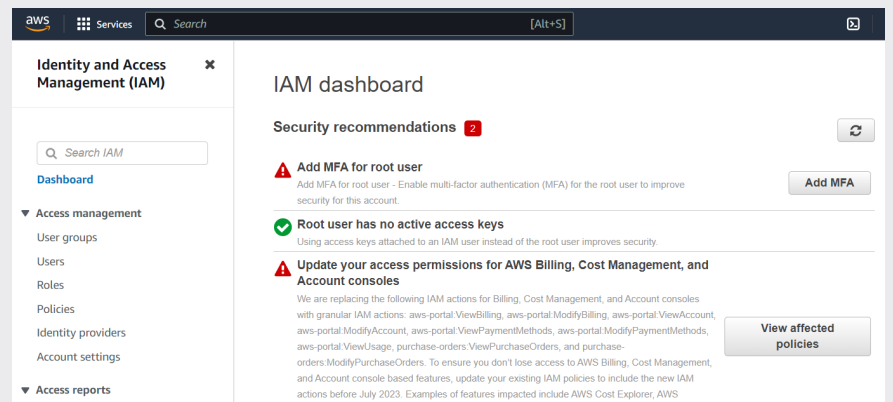
STEP-BY-STEP GUIDE TO SECURE SETUP

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.

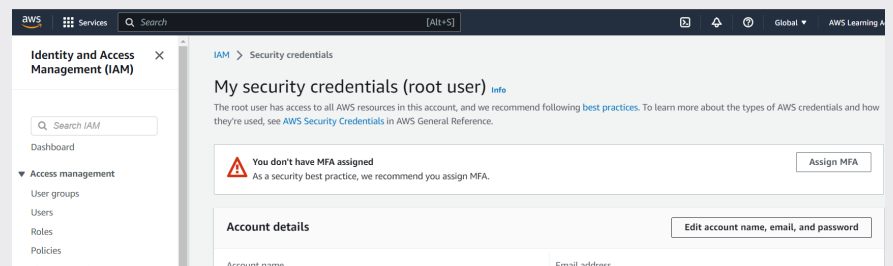
In the AWS console, open IAM



Click Add MFA



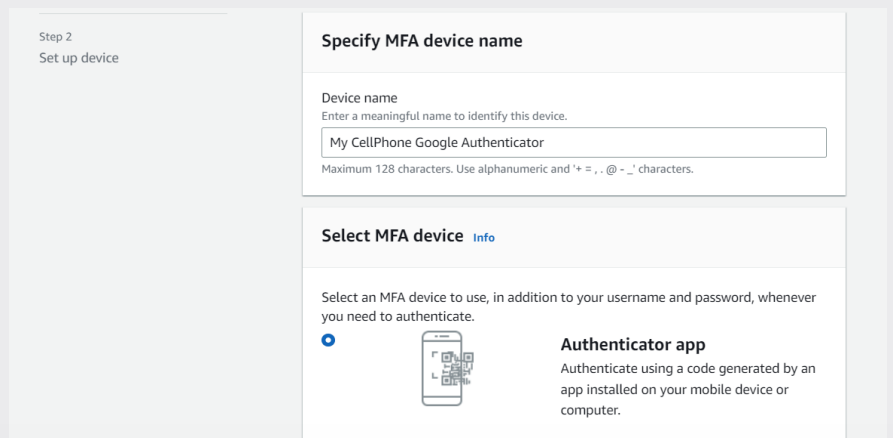
Click Assign MFA



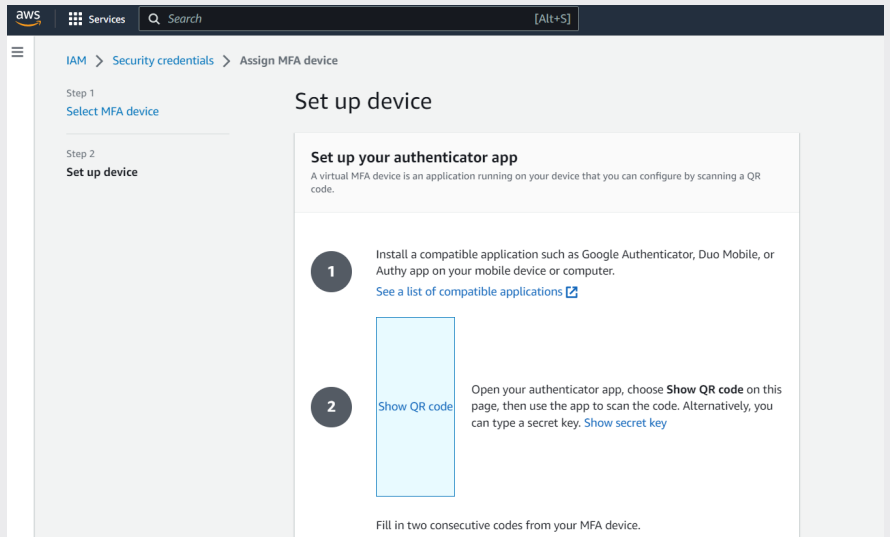
Enter a Name friendly name for the Authentication Device

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

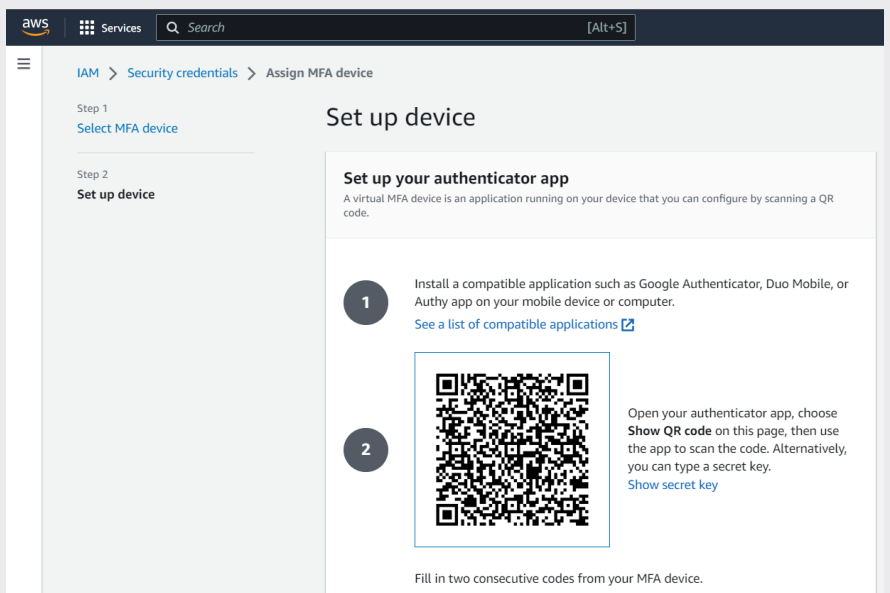
You can use any MFA software of your choosing.



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

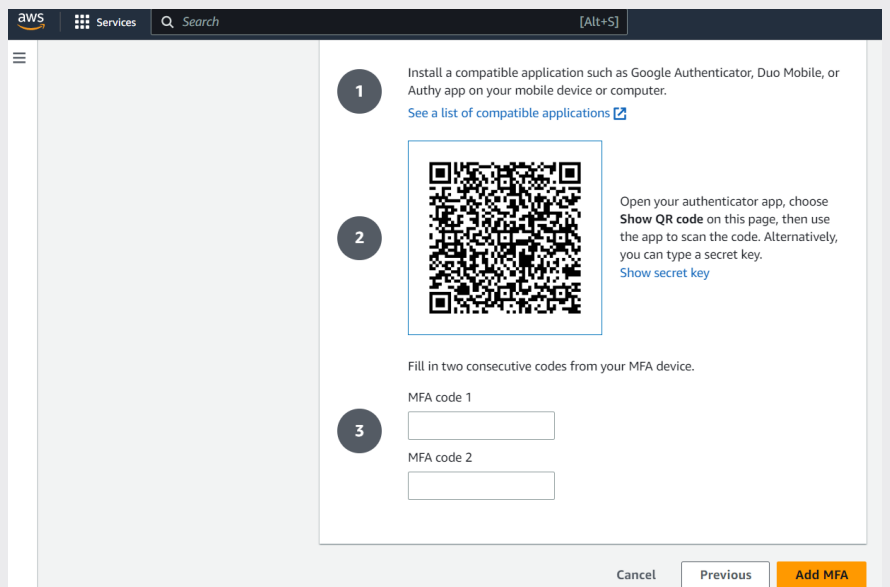


Click Show QR Code




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

Click “Add MFA”.



aws Services Search [Alt+S]

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2  Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)

3 Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

Cancel Previous **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”.



Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: 

MFA code

Submit

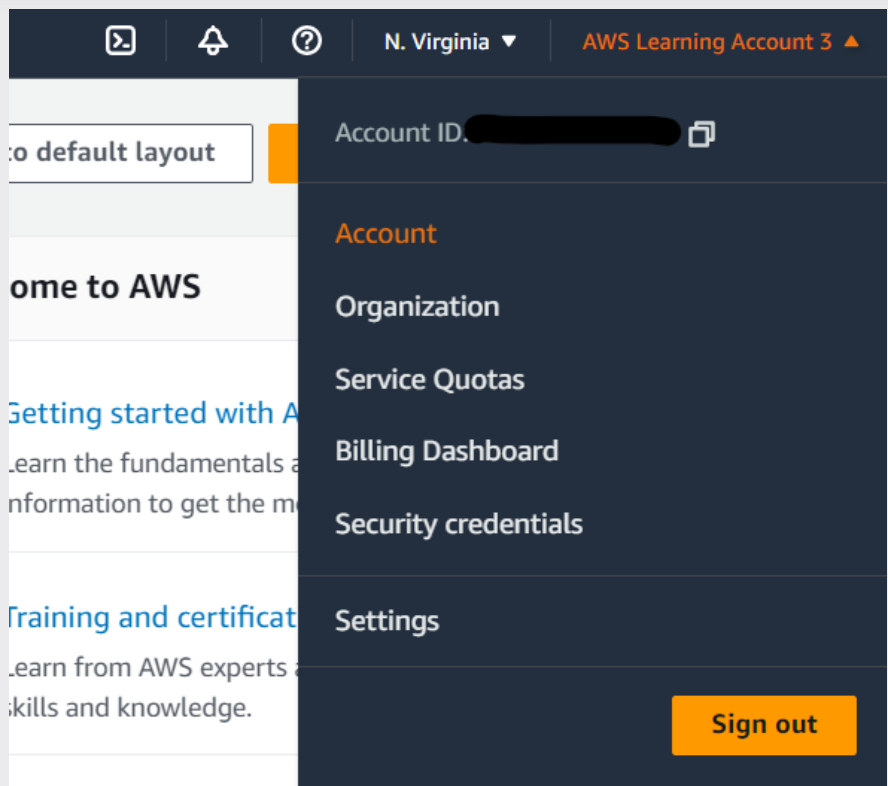
[Troubleshoot MFA](#)

[Cancel](#)

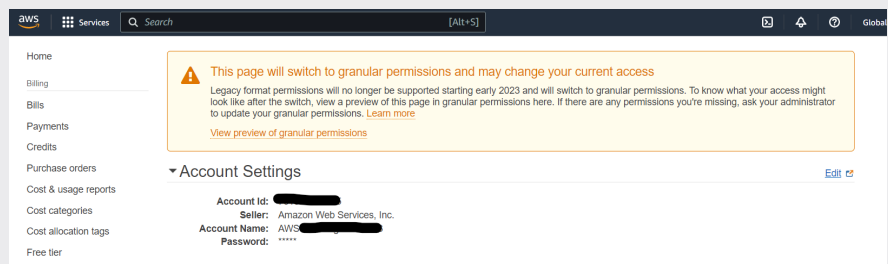
2) Use strong passwords: Ensure all users with root account access have strong passwords that meet AWS password requirements. Regularly update passwords to maintain security.

To change your root password

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



Click Edit



Click Edit Under Password

A screenshot of the 'Update account settings' form. It contains three input fields: 'Name' (with an 'Edit' button), 'Email' (with an 'Edit' button), and 'Password' (with an 'Edit' button). A blue 'Done' button is at the bottom.

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."



Update your password

Update the password for your AWS account root user.
Use the new password the next time you sign in.

Email address: wdsargent+AWS03@gmail.com

Current password

New password

Confirm new password

Save changes

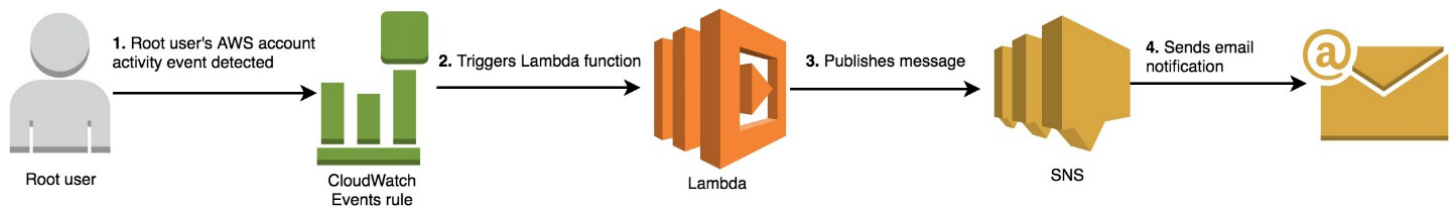
Cancel

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.



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

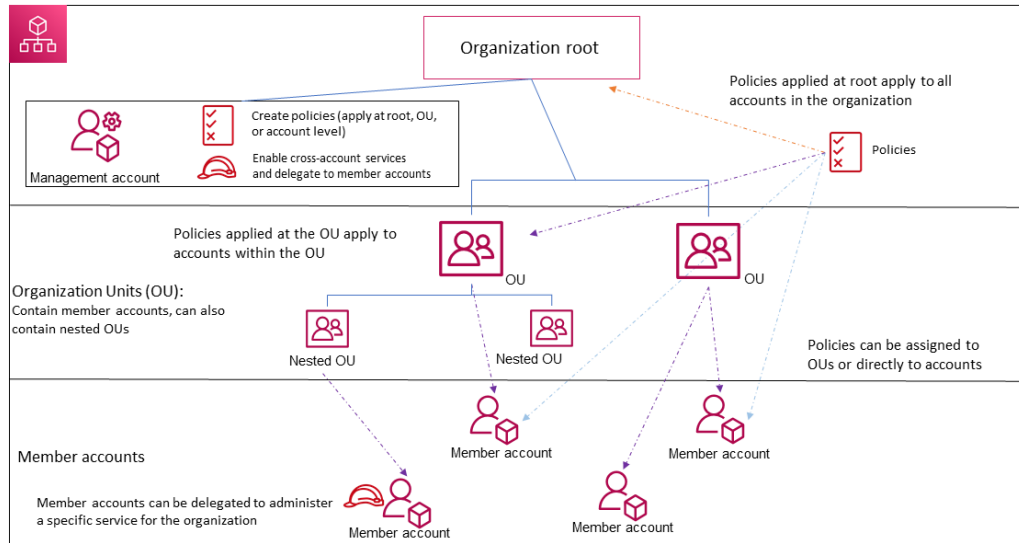
The screenshot shows the AWS IAM dashboard. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with a search bar and a 'Dashboard' link. The main content area is titled 'IAM dashboard' and features a 'Security recommendations' section with a red badge indicating 1 recommendation. Two recommendations are listed, both with green checkmarks:

- Root user has MFA**: Having multi-factor authentication (MFA) for the root user improves security for this account.
- Root user has no active access keys**: Using access keys attached to an IAM user instead of the root user improves security.

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

SDG is a leading provider of technology, consulting, and managed services that enable organizations to confidently execute cyber security, identity, and risk management solutions to mitigate risk, protect assets, and grow securely.



■ 55 North Water Street
Norwalk, CT 06854

■ 203.866.8886

■ sdgc.com