

Overview of AWS MFA:

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password. With MFA enabled, when a user signs in to an <u>AWS Management Console</u>, they will be prompted for their user's name and password (the first factor is what they know), as well as for an authentication code from their AWS MFA device (the second factor is what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

Why AWS MFA is Required:

- Users have access to your account and can possibly change configurations and delete resources in your AWS account, so to overcome this it is required
- If you want to protect your root accounts and IAM user.
- Even if the password is stolen or hacked, the account is not compromised.
- When you enable this authentication for the root user, it affects only the root user credentials. IAM users in the account are distinct identities with their own credentials, and each identity has its own MFA configuration.





MFA Device Options In AWS

The following are the MFA device options in AWS:

- Virtual MFA Device: Support for multiple tokens on a single device e.g Google Authenticator (Phone Only) Authy (Multi-Device)
- Universal 2nd Factor (U2F) Security Key: Supports multiple root and IAM users using a single security key. e.g Yubikey by Yubico (Third Party)
- Hardware Key Fob MFA Device: Provided by Gemalto (Third Party)
- Hardware Key Fob MFA Device AWS GovCloud (US): Provided by SurePassID (Third Party)

Enabling MFA on Root Account

- **1)** Log in to your AWS account.
- 2) On the right side of the navigation bar, choose your account name, and choose My Security Credentials.

		Global ▼ Support ▼
IAM dashboard		My Account e89610609184
Sign-in URL for IAM users in this accourt	nt	
https://bhanvendra.signin.aws.amazon.com	Vconsole 🖉 Edit Delete alias	My Service Quotas
IAM resources		My Billing Dashboard
Users: 0	Roles: 8	My Security Credentials
Groups: 0	Identity providers: 0	
Customer managed policies: 0		Sign Out
Security alerts		QUICKTINKS
The root user for this account does not i security for this account.	have Multi-factor authentication (MFA) enabled. Enable MFA to improve	My access key
Best practices		
 Grant least privilege access (2* Establis to perform the most minimal set of funct efficiency. 	hing a principle of least privilege ensures that identities are only permitted ions necessary to fulfil a specific task, while balancing usability and	
 Enable Identity federation: Centrally ma federation to multiple accounts in your A Sign-on. 	nage users and access across multiple applications and services. For WS Organization, you can configure your identity source in AWS Single	



3) Click on Assign MFA device.

My security credentials (root user) Info The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference. MFA not activated for root user The root user for this account does not have multi-factor authentication (MFA) activated. Activate MFA to improve security for this account.

4) Choose Virtual MFA Device and click on Continue.

Selec	t MFA device	
Speci	fy MFA device name	
Device i Enter a n ABC Maximur	name neaningful name to identify this n 128 characters. Use alphanum	device. eric and '+ = , . @' characters.
Select	t MFA device Info	
Select a	n MFA device to use, in add	ition to your username and password, whenever you need to authenticate.
•		Authenticator app Authenticate using a code generated by an app installed on your mobile device or computer.
	<i>P</i> :	Security Key Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.
0		Hardware TOTP token Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.
		Cancel Next



5) Now Install Google Authenticator on your phone.Android: <u>Click here</u>IOS: <u>Click here</u>

6) Now Click on Show QR Code and open the Google Authenticator app on your phone.

Set up device	
Set up your authenticator app A virtual MFA device is an application running on you	r device that you can configure by scanning a QR code.
1 Install a compatible application s Authy app on your mobile device See a list of compatible application	such as Google Authenticator, Duo Mobile, or or computer. ons 🔼
	Open your authenticator app, chose Show QR code on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key
Fill in two consecutive codes from MFA code 1	n your MFA device.
MFA code 2	
	Cancel Previous Add MFA

Note: Take a screenshot of the code so that in the future if you lose your phone, you can use it to re-enable MFA.



7) Now open the Google Authenticator App Click on Get started and scan the QR code.



- 8) Now enter the code from your Phone into MFA code 1 and MFA code 2.
- 9) After adding MFA code click on Assign MFA.





Identity and Access Management (IAM) the an MA later; you next a own parson and in 38 days and LANT man ж Set up virtual MFA device Change password Dashtoord You have successfully assigned virtual XFA. This virtual XFA will be required during agn-in. Access keys for CLI, S Und account keys to make pr keys plot particul reference Users. Close 2015 Conste access key Fairing. Status Created Lastunet Martly priviles. Access key II Actions Account settings Active 2028-09-30 07 04 UTC-0030 2026-10-00 23 16 UTC-0030 ARAATYQVTEGRABILPS Real Parties Rozana analyzar Multi-factor authentication (MFA) Arctive rules For increased security, we recommend carr Laters from wy Mill to help to Analyzana Saltriga Banage WA device Assagned MA device an ave are initial process standard Artual Organization activity Carriede contratt genieure (162746) X 509 certificate Q. Server Mal Use 3.500 certificates to make secure certificates periodically Laws main

10) You will get a success message then click on Close.

11) Now you will see that the device has been added for MFA.

tanagement (LCM)	Access keys for CU, SDK, &	API access			
Beahboard	One access keys to make programmy long you cannot retrieve it, leader	atic calls to Artif	5 ban the AUG Command Live In rev anteres Key and make the	erface (ADE Cu), Tools for Otro All boy Machine, Learn mere	tions ProverShell, the AMS SDKs, or shead AMS API table. If you take or Target your secret
Access management	Create atorna has				
Orage					
199.8	Access key ID	Status	Created	Lastword	Actiona
Polices	AKARTYGYITGFASFILPS	Active	2626-89-30 07 04 070-8526	2020-10-04 23:55 (/*C+0530	Make Machine Seales
sterity providers.					
Account settings	Multi-factor authentication (1	dFA)			
Access reports Access statyper	Manage MFA device	nd southparing t		The LIFA requires users to by	e a waper aufvertication code frum an agenered aufvertication device when they sign in to AVIS.
Archive rules	The second second second				
Archive tules Analyzers Settinge	Assigned MFA device an avecam: 111107273282 where	Net Cristians			
Arphive rules Analyjens Settinge Credentue report	Assigned MFA device are averally 10107273292 intern	Nen Crimologi			
Arthive rues Analytens Settings Credential report Organization activity	Assigned MPA device an area all. 11167272282 when X 509 certificate	Nan Cristian)	*		
Archive sales Analyjens Settinge Orgenigates activity Service control policies (SDPs)	Assigned MIA device an avectain: THEE225292 Intern X: 509 centRicate Use X:50 centRicate Inter X:50 centRicates	nan (1950a) 14 SOAP-politik	d-repuesta la sorre ASIS service	s. Far year protection, Altern your	private sentificate bays securary and do not share them. AVE recommends that you relate your
Archive rules Analytenis Settings Credenter equal Operation actually Service control pelices (CON)	Assigned MIA device an average 11107272202 intern X 509 certificate lise X 50 certificate certificate periodicale (see more create new certificate)	nan Cristiaa) 19 SCAP asratan Pload your me	e resuestà la same AVE service n certificate	. Par yaar protection, Allera yaar	private softRidde keys security and do not share them. AV/3 recommends that you relate your
Anthre rules Analyses Settings Ondermaingont Organization activity Service control protons (CDN) Dr. Swent VAL	Assigned MPA device and avoid also: THIRD 2020 States X: 500 CentRicate Use X:50 CentRicate Use X:50 CentRicates Create new centRicate Create new centRicate	han (195ad) • 30AP aresto pload your ree	e resuests to some AVE service in nertificate	n Par yaar protection, Allera yaar	private semplicate key's security and do not after them. AVVS recommends that you relate your.

12) Now you have successfully Activated MFA on your root account setting.

MRT FRANKLINS

Accessing AWS Console Using MFA:

1) Open your AWS console login page and click on Root User then enter your email.



Sign in



Account owner that performs tasks requiring unrestricted access. Learn more

◯ IAM user

User within an account that performs daily tasks. Learn more

Root user email address



By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

Create a new AWS account



2) Enter your password corresponding to the Email address.



Root user sign in o

Email:	
Password	Forgot password?
Sign in	
Sign in to a different account	

Create a new AWS account

3) Use your **Google Authenticator** Application on mobile and enter MFA code in AWS Console.



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.

MFA code	
695768 -	
	Submit
Troubleshoot MFA	
Cancel	

CONGRATULATION. You've set up AWS MFA and enable it.