

#1 Task: Have a look at the Cloud expenses from Cost Explorer regularly. Also, enable MFA for the AWS Root User.



Cost Analysis Tools on AWS

We will explore some of the AWS tools which can be used to understand the cost and also create some notifications-based alerts to tame the usage of the AWS services.

- Cost Anomaly Detection
- AWS Cost Explorer
- AWS Budget
- AWS Cost and Usage Dashboards

Cost Anomaly Detection

AWS Cost Anomaly Detection is a monitoring feature that utilizes advanced machine learning techniques that identify anomalous and suspicious spend behaviors as early as possible so we can avoid costly surprises. Based on the selected spend segments, Cost Anomaly Detection automatically determines patterns each day by

adjusting for organic growth and seasonal trends. It triggers an alert when spend seems abnormal.


Cost Anomaly Detection summary

Anomalies detected (MTD)	Total cost impact (MTD)	Total spend (MTD)	Total spend (vs. last month)
1	\$0.53	\$179.16	-54%

Detection history | Cost monitors | Alert subscriptions

Detection history (1) [Info](#)

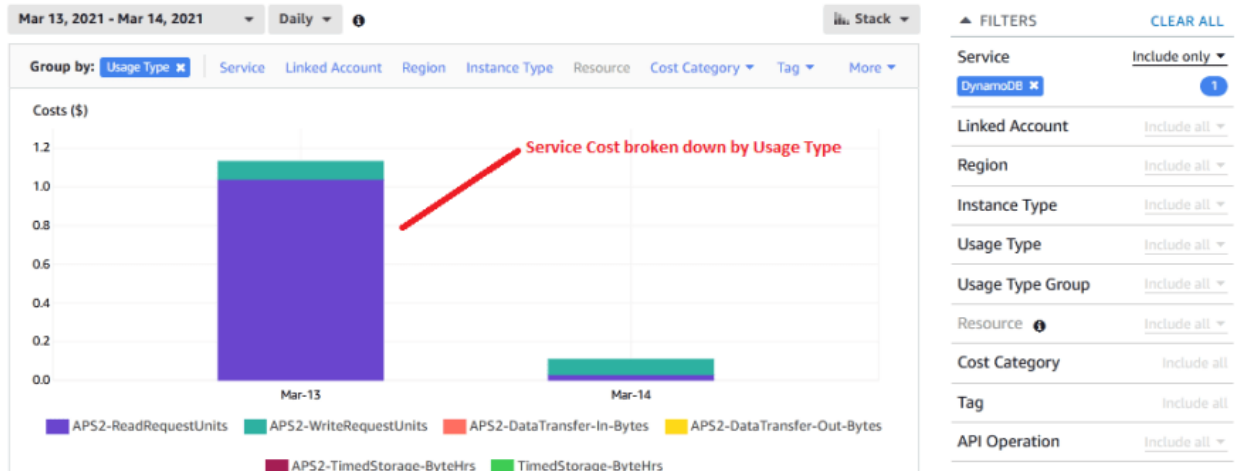
Last 90 days (all) < 1 > ⚙️

Detection date ▲	Severity ▼	Duration	Monitor name	Service	Account ID	T
2022-03-05	Low	1 day	CostAnomalyDetector	Amazon Elastic Container Service		

AWS Cost Explorer

The Cost Explorer provides us with granular insight into the AWS service usage and costs accrued. It gives us a detailed breakdown of all services in the table view & visually. We can get AWS costs and usage over a daily or monthly granularity. It gives us the capability to create reports.

With granular insights, we can identify services and usage types that are costing more. It also helps us visualize cost trends over time. We can look for any sudden spike in usage.



AWS Budget

Sitting alongside each other within the AWS Cost Management group, AWS Budgets and AWS Cost Explorer are complementary services from Amazon Web Services (AWS). Using them together, we can analyze our cost and usage patterns and use that analysis to implement effective governance controls and cost optimizations. AWS Budgets lets us track service usage, utilization, and coverage for Reserved Instances and Savings Plans.

Creating budgets

There is an AWS setup wizard that starts when we create a budget through the console. Within the wizard, there are "Info" links at the top of each page, which lead to more detailed instructions and AWS documentation.

Budget alerts

Alerts are attached to a budget and can be created when creating or editing that budget. They consist of a threshold and a notification. The threshold contains a trigger, which determines whether the alert fires when today's actual usage or the forecast usage for the budget period crosses the threshold.

We can also configure alerts to trigger automated actions when they fire. An action can be one of:

1. Attach an IAM policy to a user, group, or role.

2. Attach a Service Control Policy (SCP) to an Organizational Unit or the organization's root.
3. Stop specific EC2 or RDS instances.

Forecasting in AWS Budgets

Forecasting gives us an additional option for how we set up our alerts. Using actual spending, we might set up an alert to notify us at 80% of our monthly budget, say. Using forecasting, we might want an alert based on projected overrun, say 105%. We can use both types of alerts with the same budget — a budget will support up to 5 alerts.

Limitations :

1. Forecast alerts won't fire at all unless we already have enough (roughly 5 weeks) usage data.
2. As with any forecasting, although there will be some intelligence in the underlying algorithm, it's only based on our previous usage patterns and may be inaccurate.

▼ Alert #2

Remove

Set alert threshold

Threshold

When should this alert be triggered?

105

▼

% of budgeted amount ▼

Trigger

How should this alert be triggered?

Forecasted

▼

Summary:

When your forecasted usage is greater than 105.00% (31.5 Hrs) of your budgeted amount (30 Hrs), the alert threshold will be exceeded.

Budget Reports

Budget reports are sent by email on a regular cadence. AWS keeps these reports simple (the only complexity is in the budgets themselves) — for a single report we can customize:

1. Which budgets are included (we can include more than one)?
2. How often the report should be sent — daily, weekly, or monthly.
3. Who should receive the report — a list of email addresses.

Billing Console > Budgets > Reports > Edit budget report

Edit budget report

Setting a budget report

Select the subset of budgets that you would like to include in your report, define the delivery frequency, and specify your email recipients. For example, you can create a report that monitors all budgets for linked accounts belonging to a particular business unit and have that report delivered each morning to that business unit's engineering, product, and finance leaders.

Select budgets (1/1)

Filter by budget name

Budget name	Type
Amazon-Test-Budget	Cost Budget

Delivery settings

Report frequency

Daily

Email recipients

Enter full email address separated by commas

arnav.k@amazon.com

Report name

Budget report name

Your report name will be used as the subject line of your budget report email.

Amazon-Test-Budget-Report

Cancel Save

We will look into both services in more detail and see how they differ and how they can be used together.

Dimension	AWS Budgets	AWS Cost Explorer
Main use case	Governance controls	Cost analysis
Ease of use	<ul style="list-style-type: none"> Simple user interface Guided setup for reports and alerts 	<ul style="list-style-type: none"> Chart interface, with filter options Multiple built-in charts that can be adapted
Useful features	<ul style="list-style-type: none"> Regular report delivery Granular filters Alerts Automated responses 	<ul style="list-style-type: none"> Data visualization Granular filters Cost-saving recommendations Sharing reports Hourly granularity
Customization	<ul style="list-style-type: none"> Filtering Email recipients Automated responses 	<ul style="list-style-type: none"> Filtering and grouping

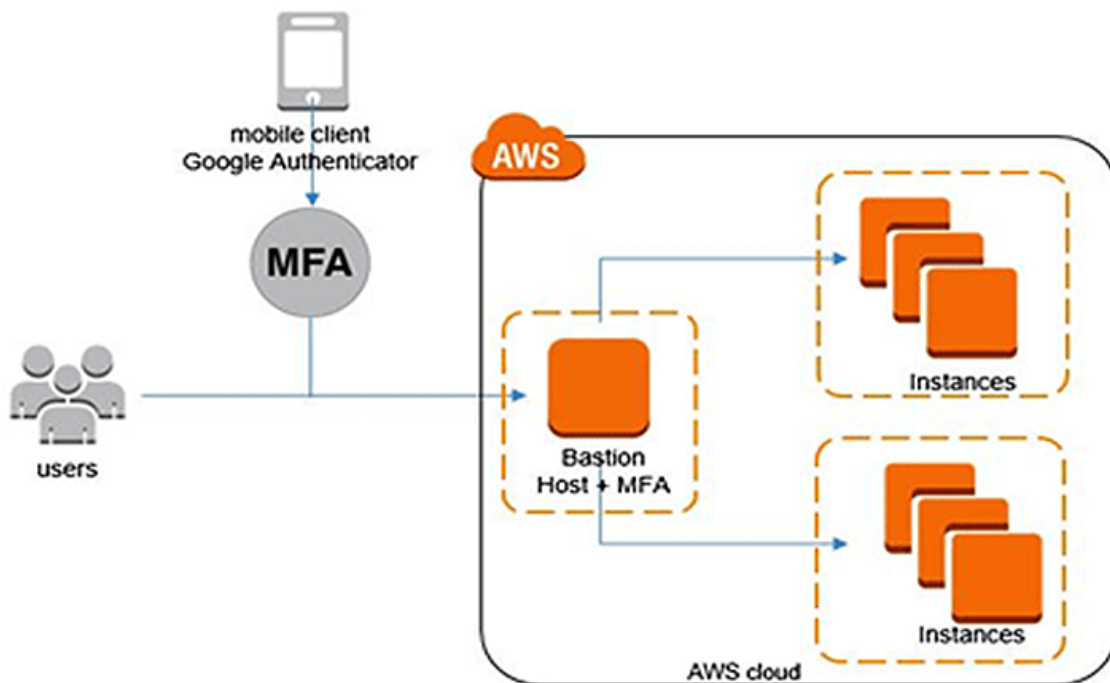
Enable MFA for the AWS Root User.

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 AWS Management Console, they will be prompted for their user 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:

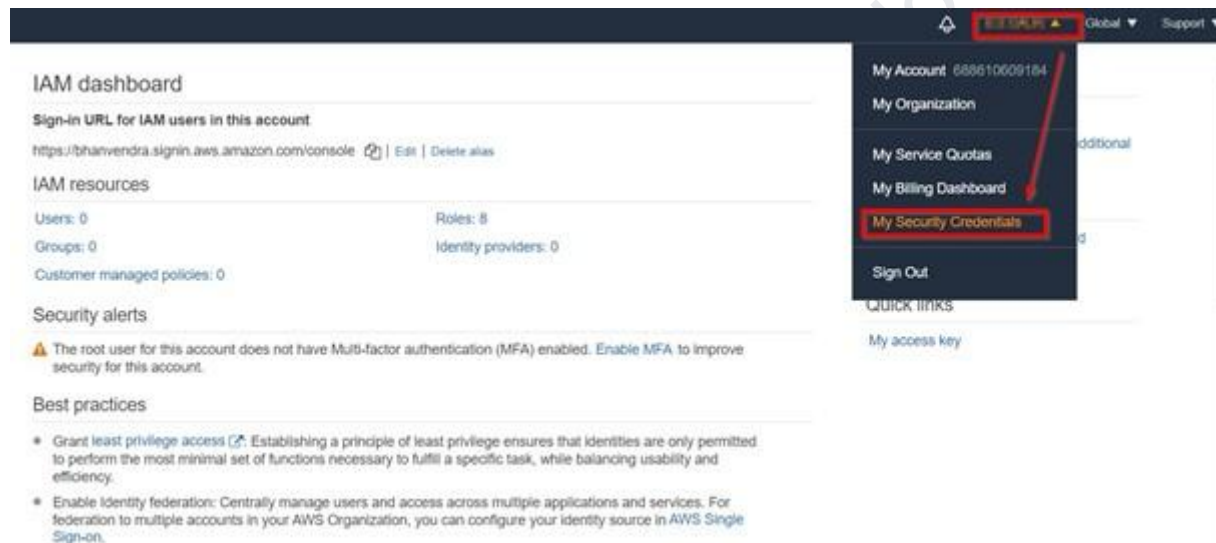
- Virtual MFA Device: Support for multiple tokens on a single device e.g Google Authenticator (Phone Only) Authy(Multi-Device)

- 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)

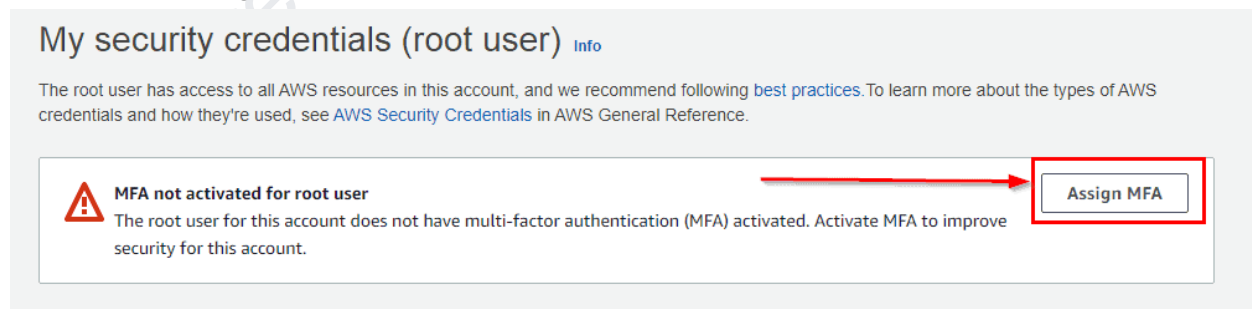
Enabling MFA On Root Account

1) Log in to your AWS account by clicking [here](#)

2) On the right side of the navigation bar, choose your account name, and choose My Security Credentials.



3) Click on Assign MFA device.



4) Choose Virtual MFA Device and click on Continue.

Select MFA device

Specify MFA device name


Device name
Enter a meaningful name to identify this device.


ABC


Maximum 128 characters. Use alphanumeric and '+ = , . @ - _ ' characters.

Select MFA device [Info](#)

Select an MFA device to use, in addition 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.

☐  **Security Key**
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

☐  **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: [Click here](#)

iOS: [Click here](#)

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 your device that you can configure by scanning a QR code.

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, 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](#)

3

Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

Cancel

Previous

Add MFA

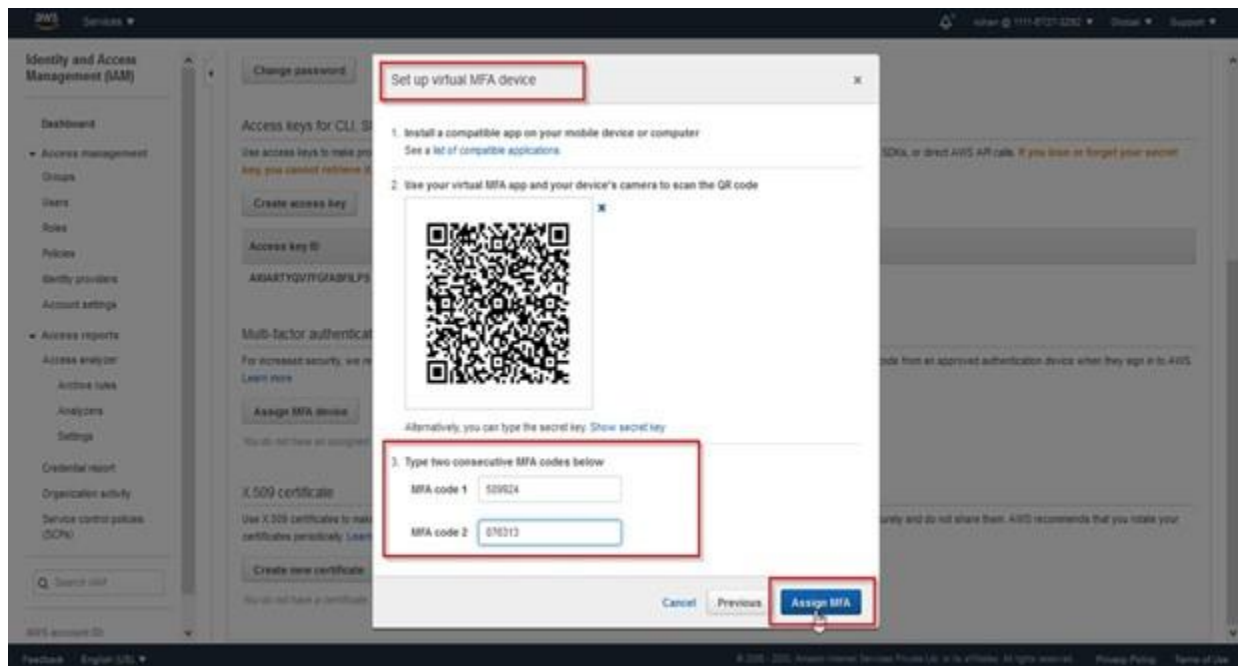
Note: Take a screenshot of the code so that in the future if you lose your phone you can use it to re-enable MFA

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

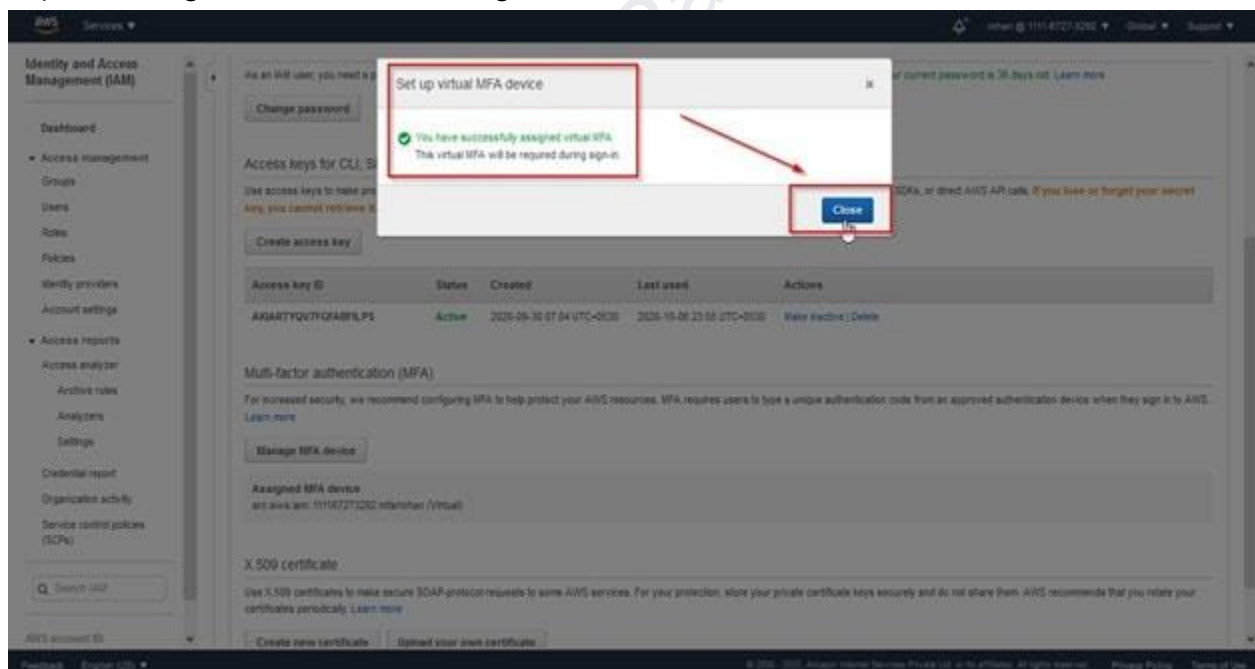


8) Now Enter the code from your Phone into MFA code 1 and MFA code 2.

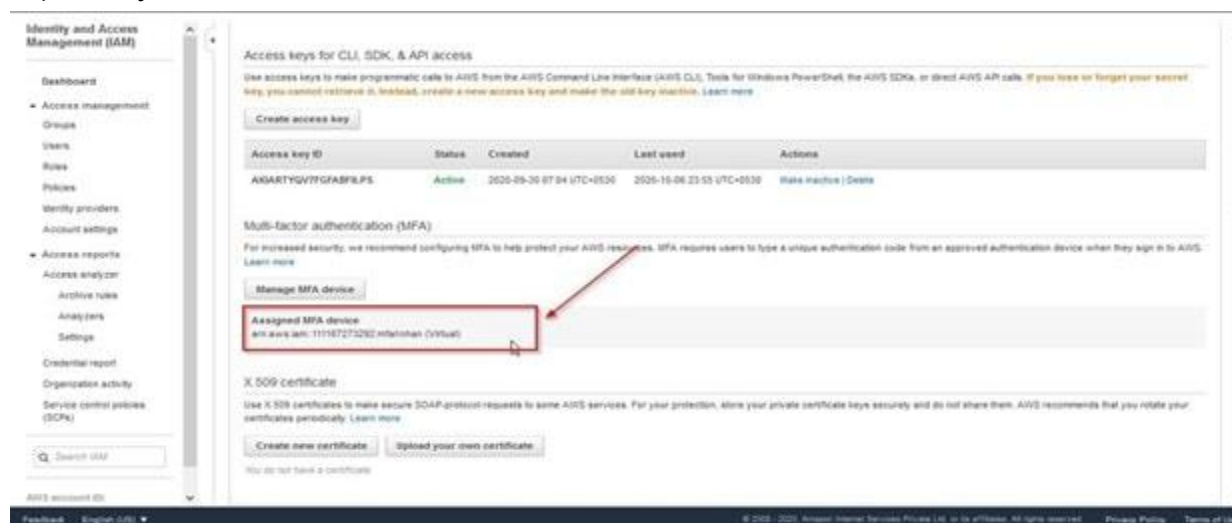
9) After adding MFA code click on Assign MFA



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



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



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

Accessing AWS Console Using MFA

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



Sign in

☒ **Root user**

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

Next

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 ⓘ

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



aws

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:
DhruvRana@gmail.com

MFA code
695768

Submit

[Troubleshoot MFA](#)
[Cancel](#)

So this was an overview of AWS MFA and how you can enable it.

What if the MFA device does not work?

If your virtual MFA device or hardware MFA device appears to be functioning properly, but you cannot use it to access your AWS resources, it might be out of synchronization with AWS. For information about synchronizing a virtual MFA device or hardware MFA device, resynchronize your virtual and hardware MFA devices.

If your AWS account root user multi-factor authentication (MFA) device is lost, damaged, or not working, you can recover access to your account. IAM users must contact an administrator to deactivate the device.