



## MFA DELETE FOR S3 BUCKET

1. In this lab you are going to enable MFA (multi factor authentication) for your bucket.
2. When the MFA is enabled, you cannot delete your bucket.
3. To do so, first you need to verify your account with MFA.
4. For that go Security Credentials of your AWS account.
5. There you will see the option for MFA.
6. Click on assign MFA device.

**Multi-factor authentication (MFA) (0)**

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Device type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
<a href="#">Assign MFA device</a>			

7. Here you have 3 options to create your MFA. But the easiest option is by using authenticator app.

**MFA device name**

**Device name**  
Enter a meaningful name to identify this device.  
  
Maximum 128 characters. Use alphanumeric and '+ = , . @ - \_' characters.

**MFA device**

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](#)

8. It will ask you to scan this QR code by your mobile device after you have downloaded the Authenticator app.
9. Scan this and add the MFA code 1 and 2. Then click on add MFA

## Set up device Info

**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, 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](#)

10. Once it is done it will look like this in your security credentials.

**Multi-factor authentication (MFA) (1)**  
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Device type	Identifier	Certifications	Created on
Virtual	arn:aws:iam::678586570493:mfa/techsup4000	Not Applicable	Now

11. Now you also need to create Access keys because you are going to use command prompt on your local system.
12. Once your access keys are created, configure them at Command prompt.

Access keys (1)					
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. <a href="#">Learn more</a>					
Actions ▾		Create access key			
Access key ID	Created on	Access key last used	Region last used	Service last u:	
AKIAZ37XJK367FDEDO54	3 minutes ago	None	N/A	N/A	

```
C:\Users\      >aws configure
AWS Access Key ID [*****5BGP]: AKIAZ37XJK367FDEDO54
AWS Secret Access Key [*****NSvL]: zqLh2cIMj4a/XPzmGH3/nwb0m5DNU8DvDp3j+6Nn
Default region name [ap-south-1]:
Default output format [None]:
```

13. Now as an example you are going to use a bucket of your choice.
14. Go and look at the objects that it has.

Buckets (2) <a href="#">Info</a>					
Buckets are containers for data stored in S3. <a href="#">Learn more</a>					
Actions		Copy ARN	Empty	Delete	Create bucket
<input type="text"/> Find buckets by name <span style="float: right;">&lt; 1 &gt; ⚙</span>					
Name	AWS Region	Access	Creation date		
appbucket8000	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	August 20, 2023, 18:06:22 (UTC+04:00)		
appbucket9000	Asia Pacific (Singapore) ap-southeast-1		August 20, 2023, 18:07:17 (UTC+04:00)		

15. There should be some objects in place.

16. Now you need to run a code in command prompt. So, you need to make some changes in this code.
17. First is to use your own ARN then in the last use your code which is showing in your MFA app. The number highlighted in the red is authenticator code.

**// This command is used to enable MFA-Delete for a bucket**

```
aws s3api put-bucket-versioning --bucket appbucket8000 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::678586570493:mfa/AWS4000
```

027317"

```
C:\Users\alash>aws s3api put-bucket-versioning --bucket appbucket8000 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::678586570493:mfa/AWS4000 027317"
```

18. If you want to confirm that MFA delete is enabled or not use this command.

**// This command is used to confirm that MFA-Delete has been enabled for the bucket**

```
aws s3api get-bucket-versioning --bucket appbucket8000
```

```
C:\Users\alash>aws s3api get-bucket-versioning --bucket appbucket8000
{
    "Status": "Enabled",
    "MFADelete": "Enabled"
}
```

19. In S3 if you go back to any of your object which you have and look at the version of it then it has only one.

20. Now you need to upload this file again so, that it two versions.

01.sql [Info](#)

Copy S3 URI Download Open Actions ▾

Properties Permissions Versions

Versions (1)

Download Open Actions ▾

< 1 >

	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	null (Current version)	sql	August 20, 2023, 18:06:56 (UTC+04:00)	253.0 B	Standard

21. Now you can see that it has two versions now.

01.sql [Info](#)

Copy S3 URI Download Open Actions ▾

Properties Permissions Versions

Versions (2)

Download Open Actions ▾

< 1 >

	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	WVj6gOFJLMoGo2WmXPvXa5WleDcPoHD1 (Current version)	sql	August 23, 2023, 14:07:43 (UTC+04:00)	221.0 B	Standard
<input type="checkbox"/>	└ null	sql	August 20, 2023, 18:06:56 (UTC+04:00)	253.0 B	Standard

22. So, now if you will try to delete this version, you will get denied. Because MFA delete has been activated.

Amazon S3 > Buckets > appbucket8000 > 01.sql > Delete objects

### Delete objects [Info](#)

✖️ You can't delete object versions because Multi-factor authentication (MFA) delete is enabled for this bucket.  
To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

[Cancel](#)

23. Now you need to run this command below to delete this object. Here you need to give the name of the bucket then what is its version ID and what is the object then your ARN and lastly your authenticator code.

// This command is used to delete an S3 object

```
aws s3api delete-object --bucket appbucket8000 --key 01.sql --version-id SgxSA0TxrFfLTH80dY0QhNfSKNufV2X6 --mfa "arn:aws:iam::678586570493:mfa/AWS4000 303684"
```

24. Once you have run the code you get this as your output.
25. And now if you go back to your bucket to see and refresh your page.

```
{  
  "VersionId": "WVj6gOFJLMoGo2WmXPvXa5WIeDcPoHD1"  
}
```

26. Here you can see that it has been deleted.

<input type="checkbox"/>	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	null (Current version)	sql	August 20, 2023, 18:06:56 (UTC+04:00)	253.0 B	Standard

27. Now if you want to disable the MFA delete you can do that by writing this command-to-command prompt.

```
// This command is used to disable MFA-Delete for a bucket
```

```
aws s3api put-bucket-versioning --bucket appbucket8000 --versioning-configuration Status=Enabled,MFADelete=Disabled --mfa "arn:aws:iam::678586570493:mfa/AWS4000 236192"
```