

AWS EC2

Demo Document 7

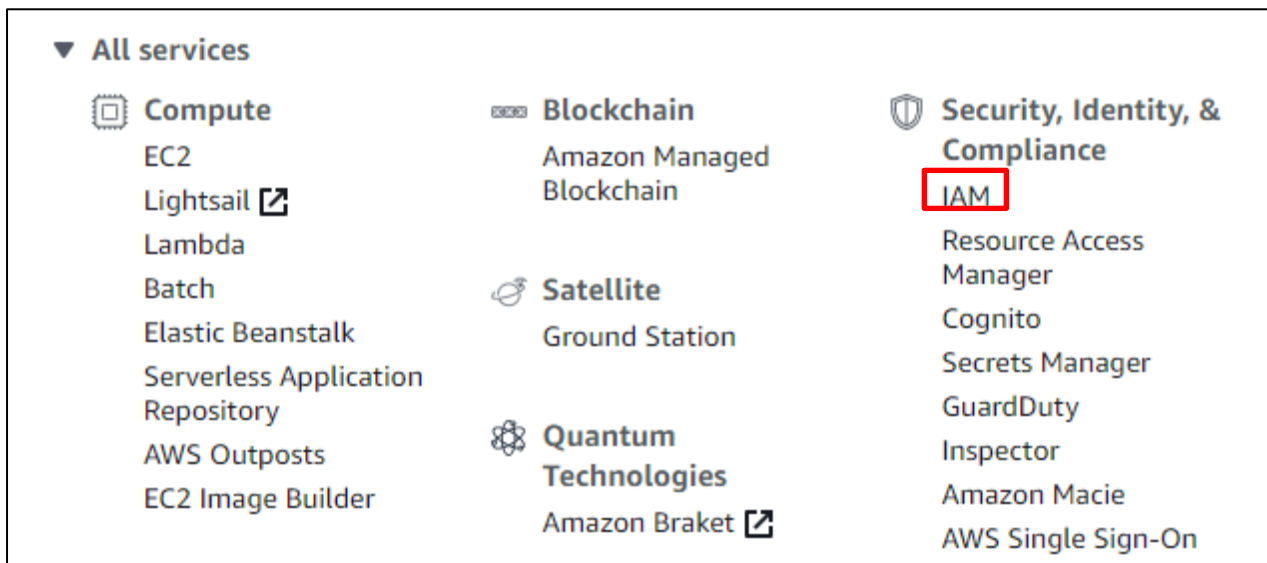
edureka!

edureka!

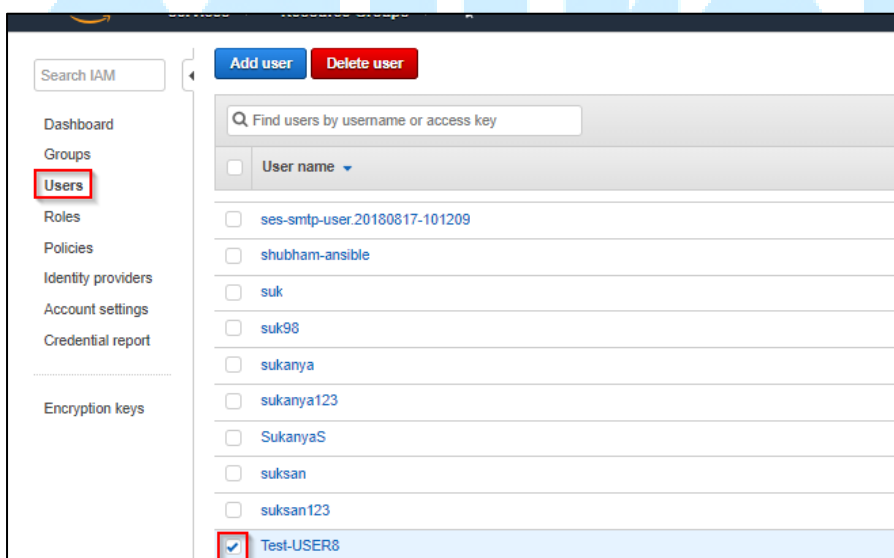
© Brain4ce Education Solutions Pvt. Ltd.

Login to AWS Console via MFA

Step 1: Go to the AWS Management Console and select AWS services. Under the Security, Identity & Compliance, click on IAM.



Steps 2: Go to **Users** and select the user who you want to enable the MFA for.



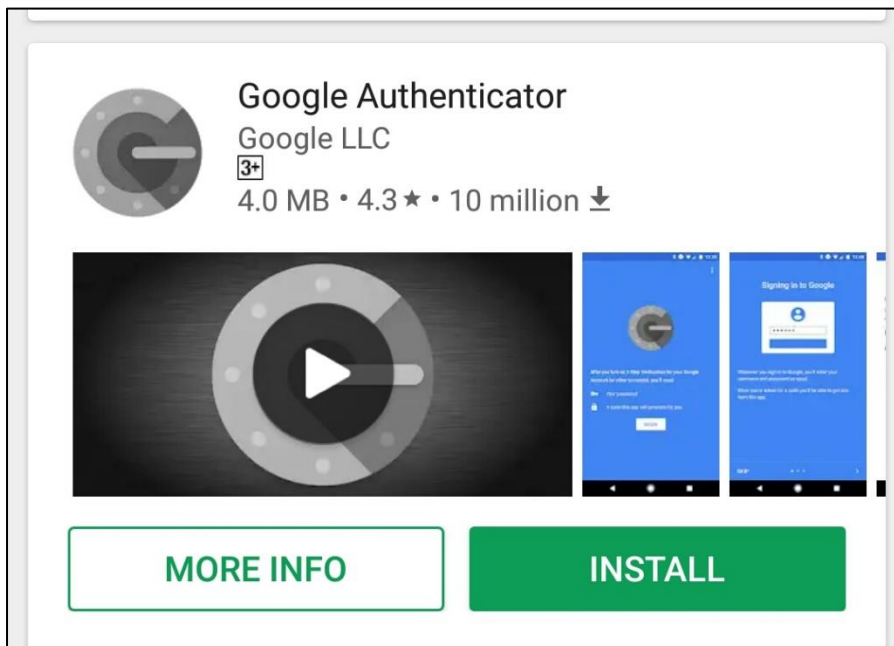
Step 3: Go to users under **Security Credentials** tab and change the status of **Assigned MFA device**

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main area is titled 'Users > Test-USER8' and 'Summary'. It displays user details: User ARN (am:aws:iam::245376966395:user/Test-USER8), Path (/), and Creation time (2018-08-31 18:08 UTC+0530). Below this are tabs for Permissions, Groups, Security credentials (highlighted with a red box), and Access Advisor. Under the 'Security credentials' tab, the 'Sign-in credentials' section shows: Console password (Enabled, with a 'Manage password' link), Console login link (https://edurekacloud.signin.aws.amazon.com/console), Last login (2018-08-31 18:10 UTC+0530), Assigned MFA device (No, highlighted with a red box and an edit icon), and Signing certificates (None, with an edit icon).

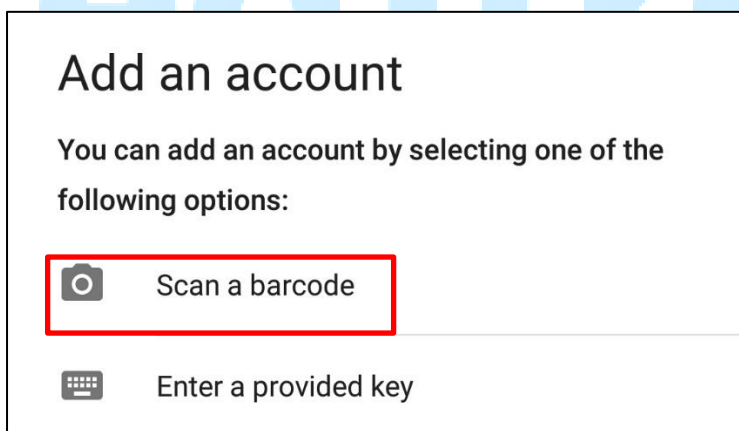
Step 4: Select **A virtual MFA device** and click on the **Next Step**.

The screenshot shows a 'Manage MFA Device' dialog box. It contains the text 'Select the type of MFA device to activate:'. Below this are two radio buttons: 'A virtual MFA device' (which is selected and highlighted with a red box) and 'A hardware MFA device'. Below the radio buttons is a link: 'For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#).' At the bottom right of the dialog are two buttons: 'Cancel' and 'Next Step'.

Step 5: Download the **Google Authenticator App** in your smartphone phone.




Step 6: Select **Scan a Barcode** and scan the barcode displayed in the AWS Management Console.



Step 7: Once the scanning is done, enter the authentication code displayed on your cell phone in the AWS Management console.

Account added

367 782


Amazon Web Services (test@edurekacloud) 

When you're asked for a verification code, find it here. The code changes frequently, so there is no need to memorise it.

ADD ACCOUNT

Account added

367 782


Amazon Web Services (test@edurekacloud) 

When you're asked for a verification code, find it here. The code changes frequently, so there is no need to memorise it.

ADD ACCOUNT

Manage MFA Device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.



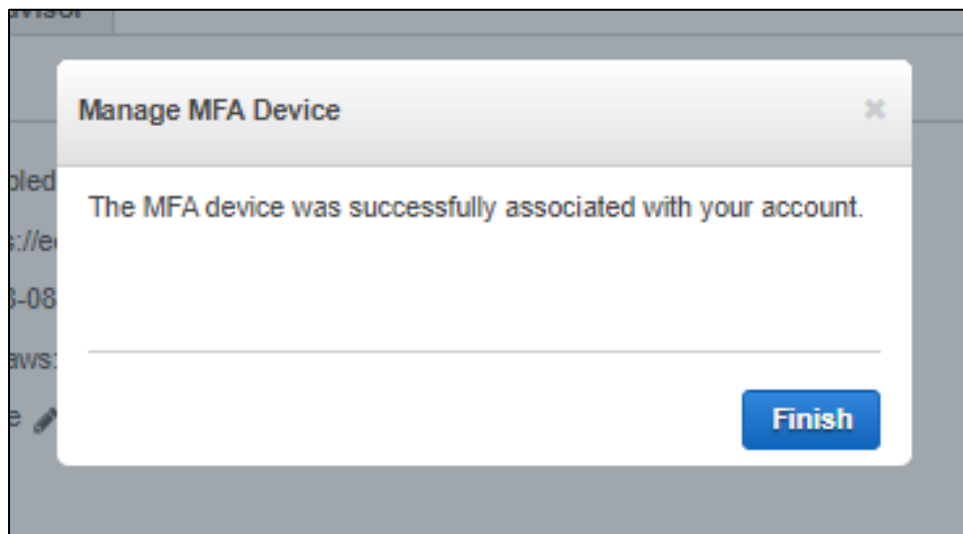
[Show secret key for manual configuration](#)
 After the application is configured, enter two consecutive authentication codes in the boxes below and choose Activate virtual MFA.

Authentication code 1
 Authentication code 2

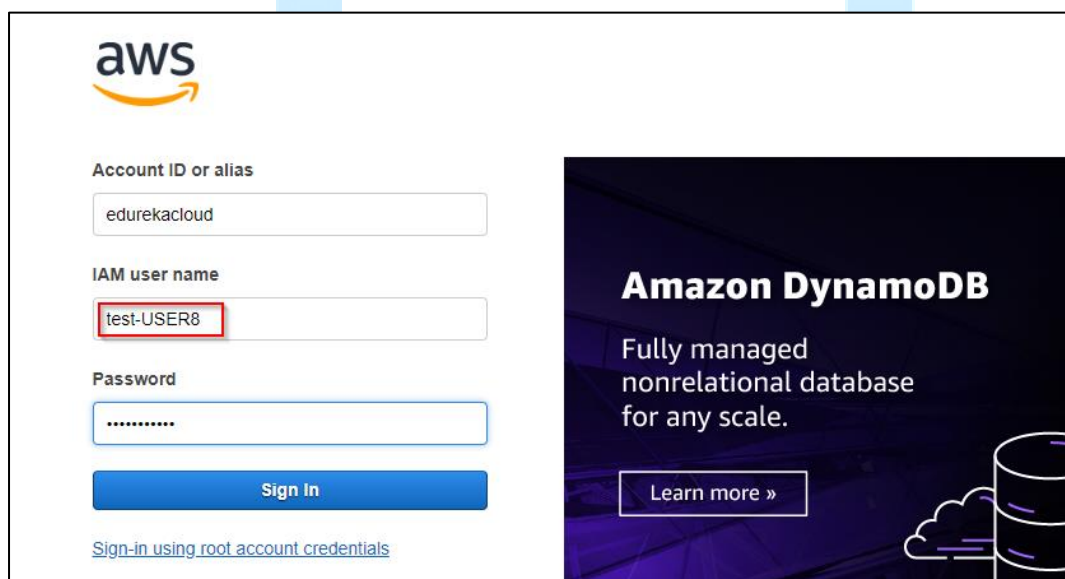
[Cancel](#)
[Previous](#)
[Activate virtual MFA](#)

eka!

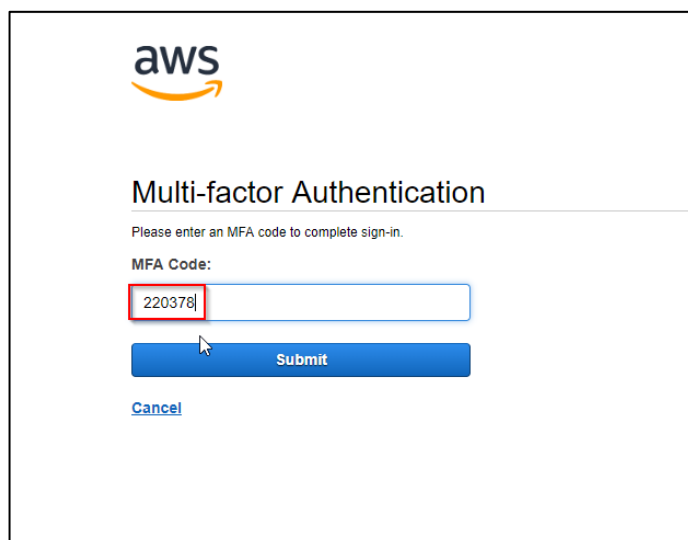
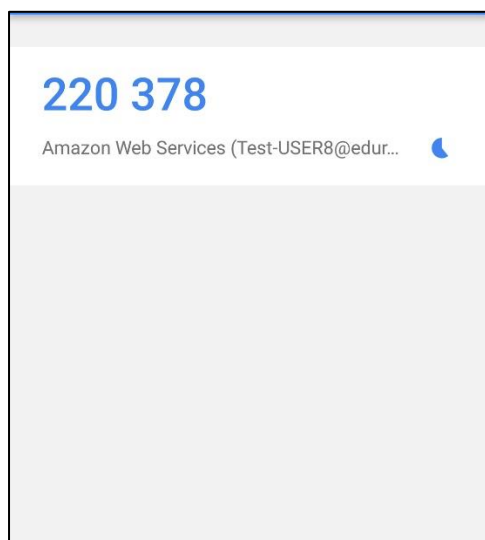
Step 8: If all the steps are in sync, it will notify you of the successful association of MFA with your account. Click on **Finish** when you see the notification.



Step 9: Log out of the current account and log in using the user to whom you have assigned the MFA.



Step 10: When prompted to enter the MFA code, enter the current code as displayed on your smartphone screen.



Conclusion:

We have successfully assigned the **MFA** to the user.