

DATE:21/02/2024

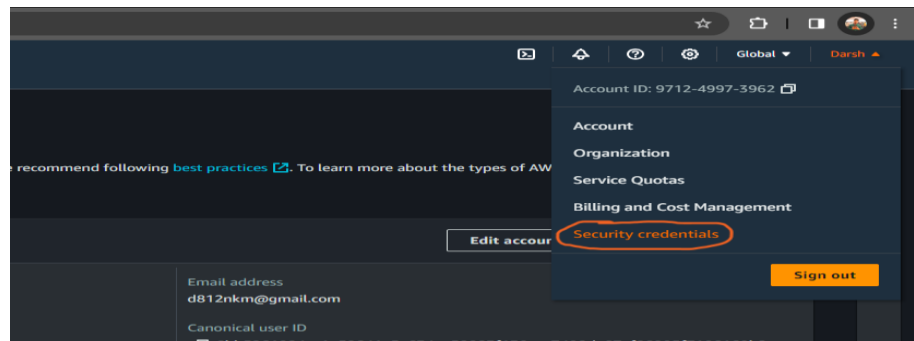
Task 1) How to set Multi-factor authentication (MFA) for AWS user

Use of MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an

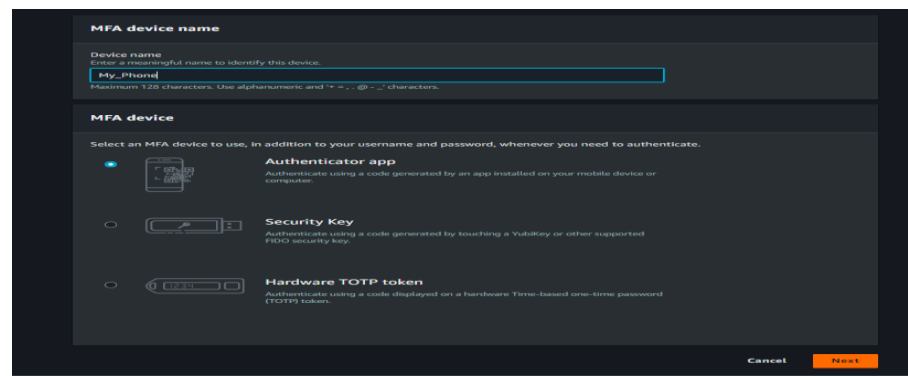
MFA device. Each user can have a maximum of 8 MFA devices assigned.

To set MFA follow the following steps (Using Authenticator App)

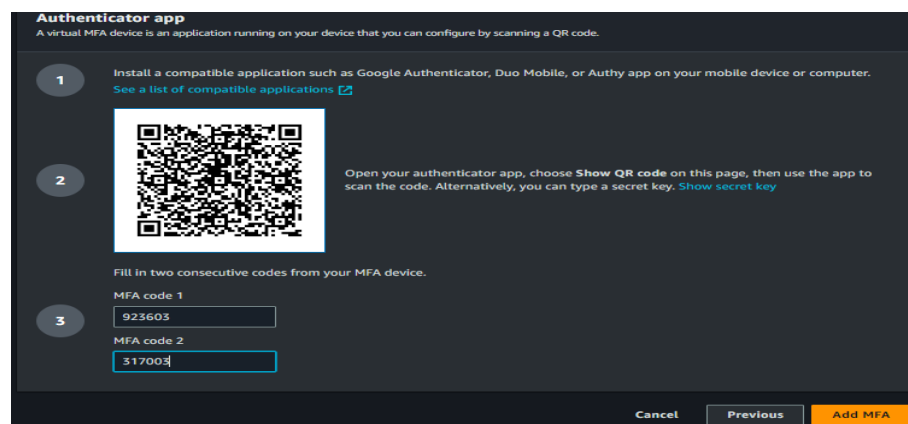
- 1) You need to download the Google Authenticator App or Microsoft Authenticator App
- 2) Sign in to the AWS Management Console
- 3) Go to IAM Service, you can simply search IAM or click on the Account info button and select Security Credentials.



- 4) Give Your Device name and select Authenticator app option then click on the next button.



- 5) Click on Show QR Code, then scan the QR code on the Authenticator App.
- 6) After Scanning QR you will get a secret MFA code in your Authenticator App, enter the code and click on Add MFA Button.

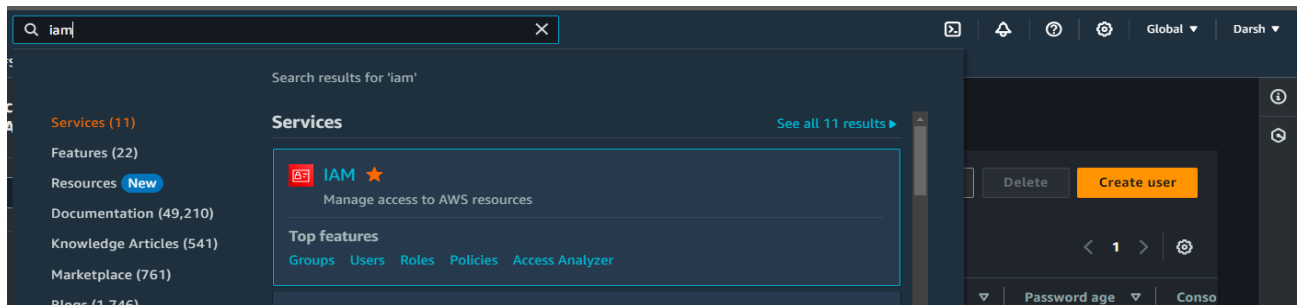


Now you will see MFA is enabled in your AWS account.

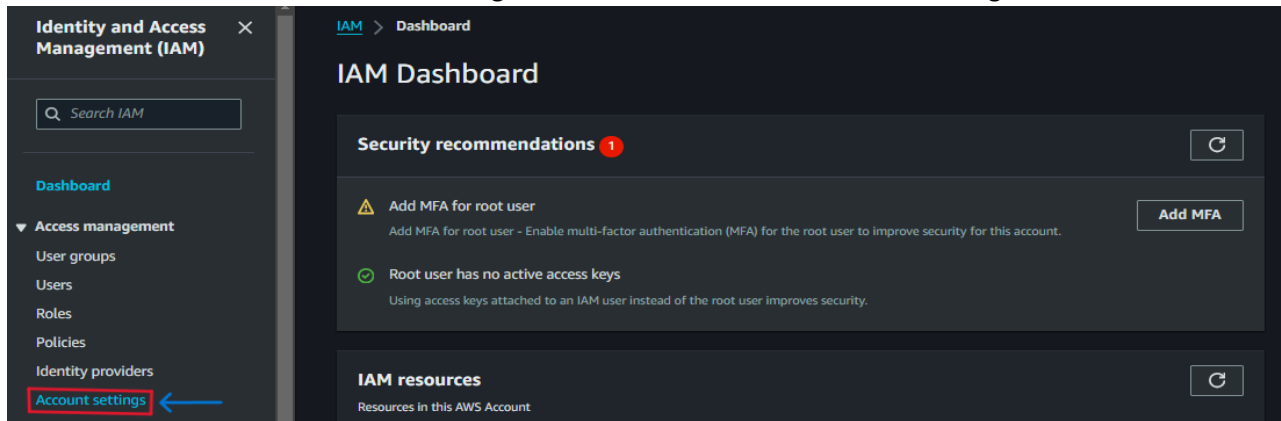
Note: To Set MFA for a Particular user Go to IAM service, select user, click on Security Credentials, then click on assign MFA Device and follow from Above 4th steps.

Task 2) Set a Custom Password Policy for Users.

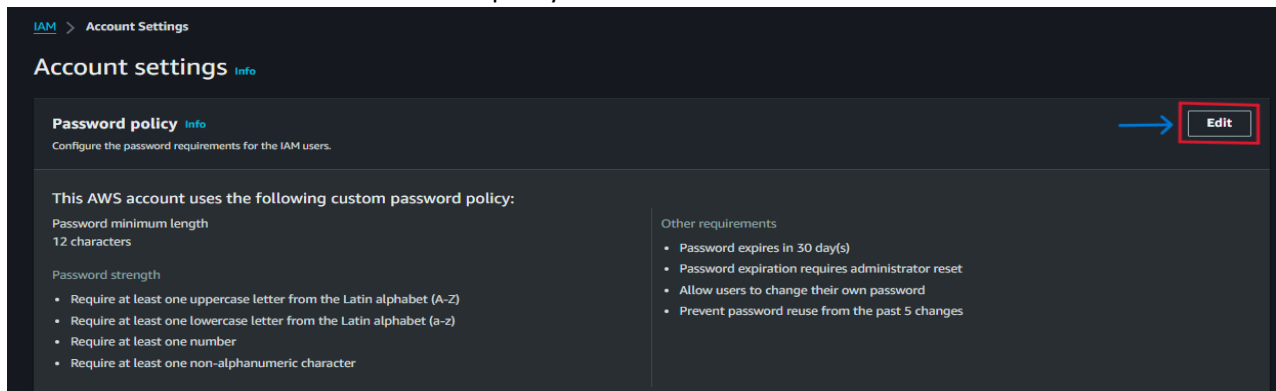
- 1) Sign in to the AWS Management Console
- 2) Go to IAM Service, you can simply search IAM, or directly search Account settings.



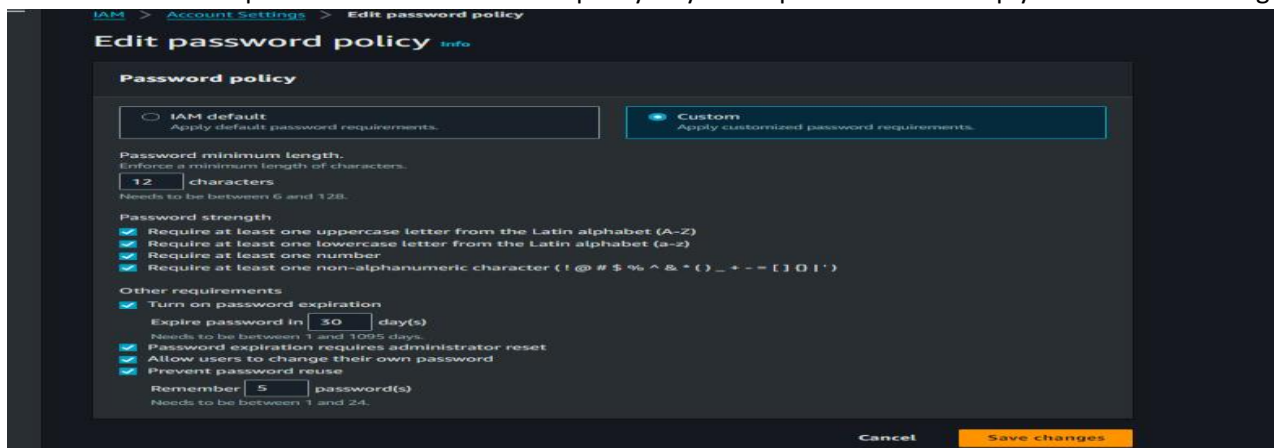
- 3) Look at the IAM dashboard Access Management Menu and click on Account Settings.



- 4) Click on the edit button of the Password policy.



- 5) Select the Custom option and set the Password policy as your requirement and simply click on Save Changes.

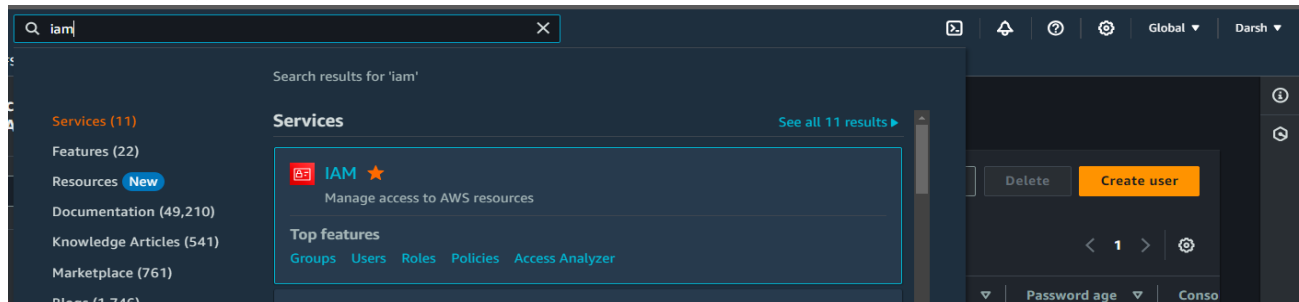


Note: This policy will impact any new user creation and all the existing users changing their passwords.

Task 3) Create IAM User in AWS Account.

Follow the following steps to create IAM user in AWS

- 1) Sign in to the AWS Management Console
- 2) Go to IAM Service, you can simply search IAM and click on it. (Also user option appears in drop up box, simply click on the user)



- 3) Then click on the Create User button and specify the user details like user name, user access, console password and check or uncheck box to the create a new password in the first login or not. After that click on next button.

Specify user details

User details

User name
Test_user
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type
☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password
☐ Autogenerated password
You can view the password after you create the user.
☒ Custom password
Enter a custom password for the user.
ABcd1234!@#
☒ Show password

☒ Users must create a new password at next sign-in - Recommended

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

- 4) Select the Permission Group that you want to give to the user or create a new Group permission, and also have the option to select existing user permissions groups and policies that you can select.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

[Create group](#)

Set permissions boundary - optional

Cancel Previous Next

- 5) After selecting Permission click on the Next Button, Review and Create page will open, carefully check the all details after creating the user, then add a tag for the user (Optional) use of a tag is to identify the user. Then simply click on the Create User Button and download your user Password file.

Now you will see the user has been created.