Force MFA:

------------------

--> Force MFA is to force the IAM user to enable MFA on their user accounts.

--> We need to create a policy which can deny all actions except the below mentioned, if there is no MFA enabled.

"iam:CreateVirtualMFADevice",

"iam:EnableMFADevice",

"iam:GetUser",

"iam:ListMFADevices",

"iam:ListVirtualMFADevices",

"iam:ResyncMFADevice",

"sts:GetSessionToken"

--> The force MFA policy is only applied if the user doesn't have MFA enabled.

1. Create an IAM user "user21" and attach the "AdministratorAccess" Policy which allows the user to perform any action.

2. Create a policy "ForceMFA" which will deny all actions except few, if there is No MFA enabled.

3. Attach the "ForceMFA" policy to the user "user21" & Login as user21 and verify the permissions.

4. Login as "user21" and enable MFA on his user account.

5. Login as "user21" and verify the permissions.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\_policies\_examples\_aws\_my-sec-creds-self-manage.html