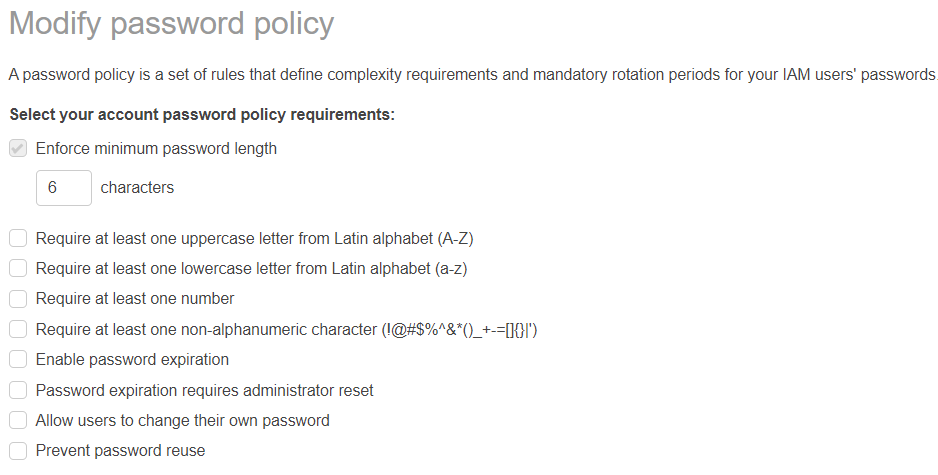
**Password policy:**

**IAM 🡪 account setting 🡪 password policy**



We can create, modify and delete the password policies here

**MFA:**

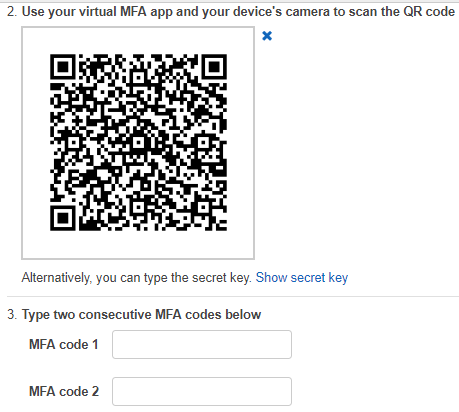
* We should add one more step for authentication
* Multi Factor Authentication (MFA). It’s just liked an OTP



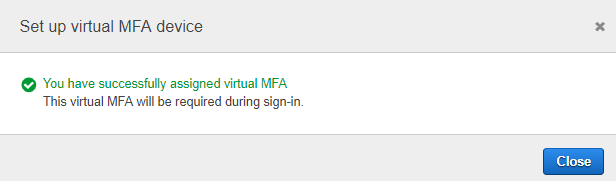
* We will get a barcode, we need to scan it with google authenticator
* Once we scan the barcode, we get a code 1 and code 2 after 30 seconds of code1
* Once this is activated, whenever user logins, he need to give the barcode along with password for authentication
* People also ask for hardware device from AWS which generates the code for authentication
* We can setup MFA root account. Activating MFA for root account is can’t be done from IAM, we need to go to my security credentials and do it
* Administrators cannot get access to billing dashboard

**Virtual MFA device:**

* Create a user with virtual MFA device



* Now scan the code from google authenticator
* And enter the two codes given by authenticator app and setup the MFA device



* After then the app keeps generating the code. So, from next login we need to enter the code along with password to login to the console

