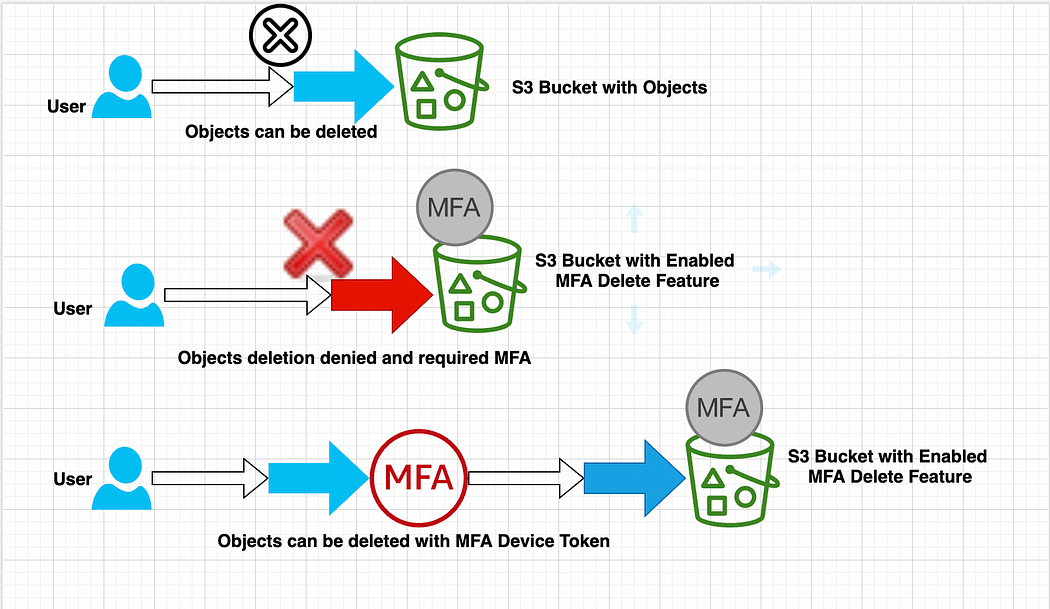
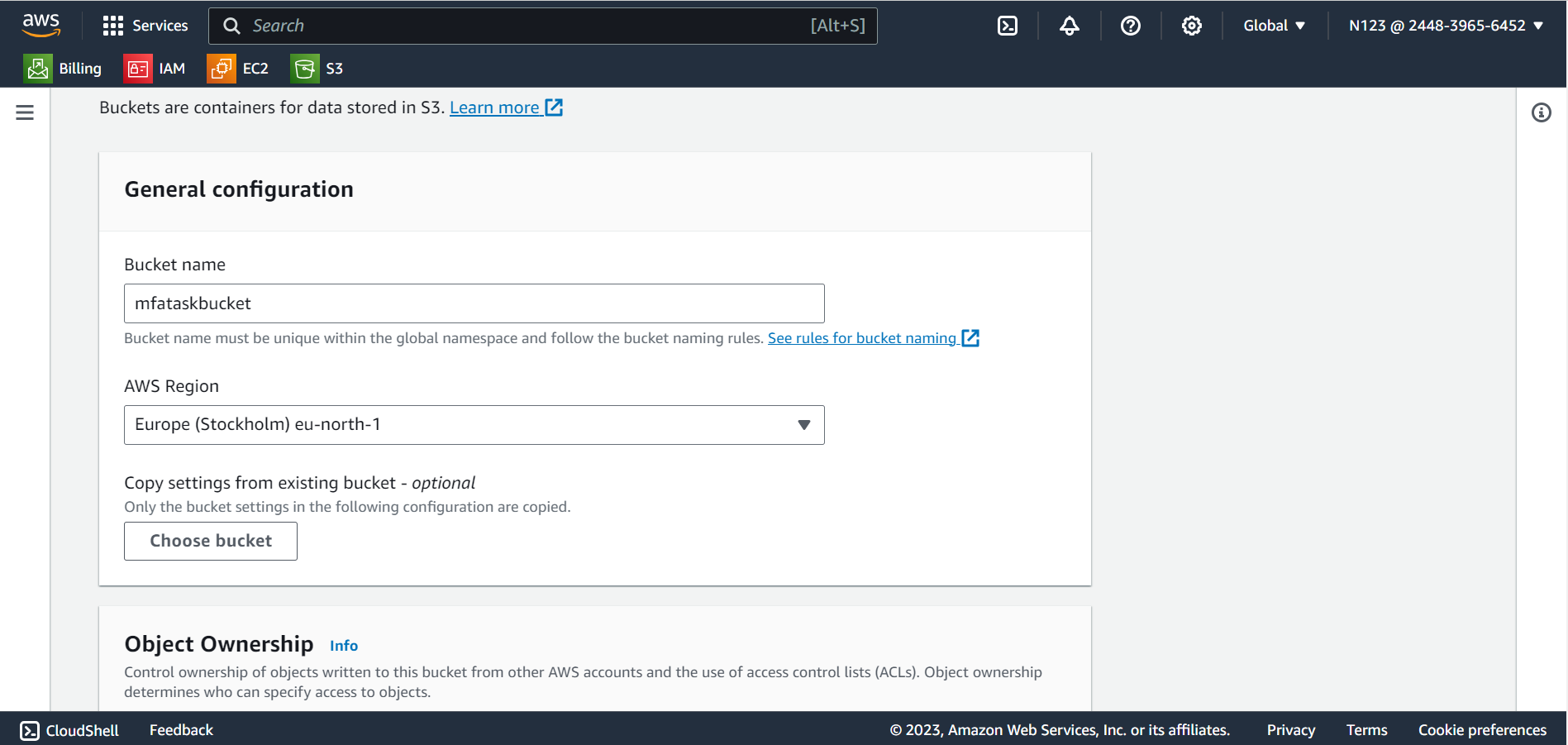
TASK 1:- Implement MFA on Bucket when users are going to delete any objects, then he needs an Approval from MFA Code



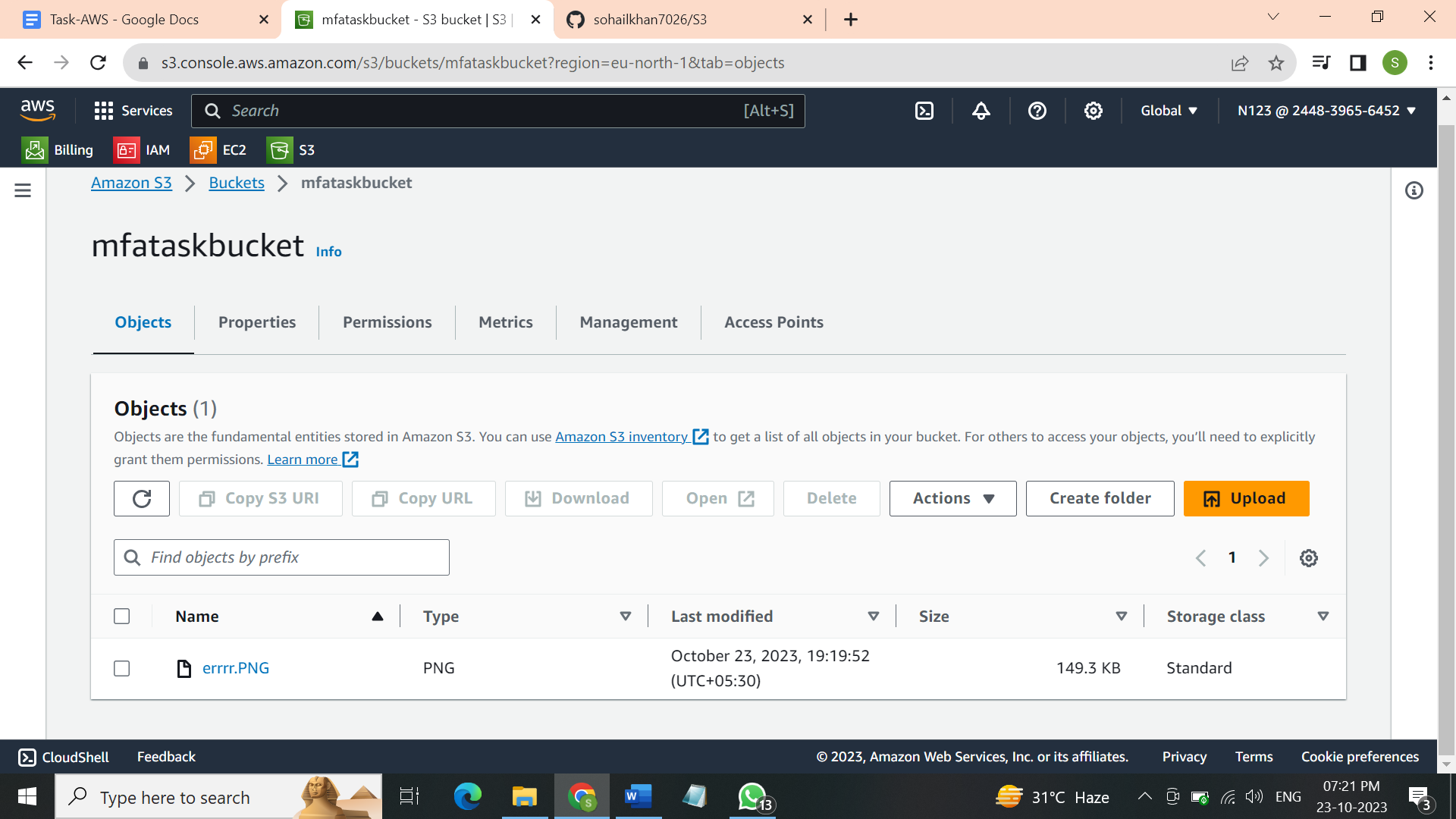
🡪 Step 1: Create Bucket

S3 --- Create bucket --- Give unique Bucket name --- Bucket region ---- Enable Bucket Versioning(not allowed to enable Mfa without this) --- Create bucket



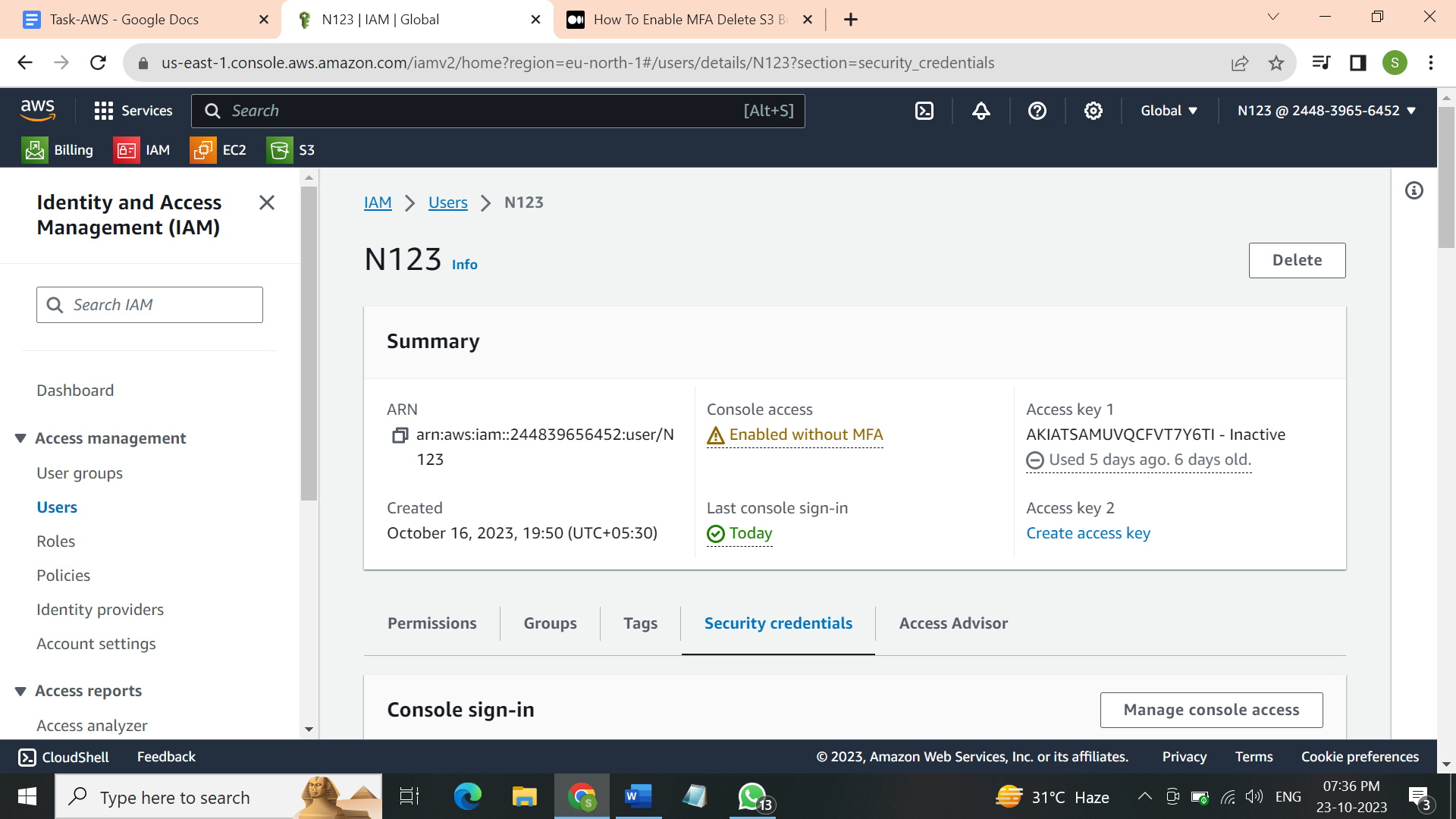
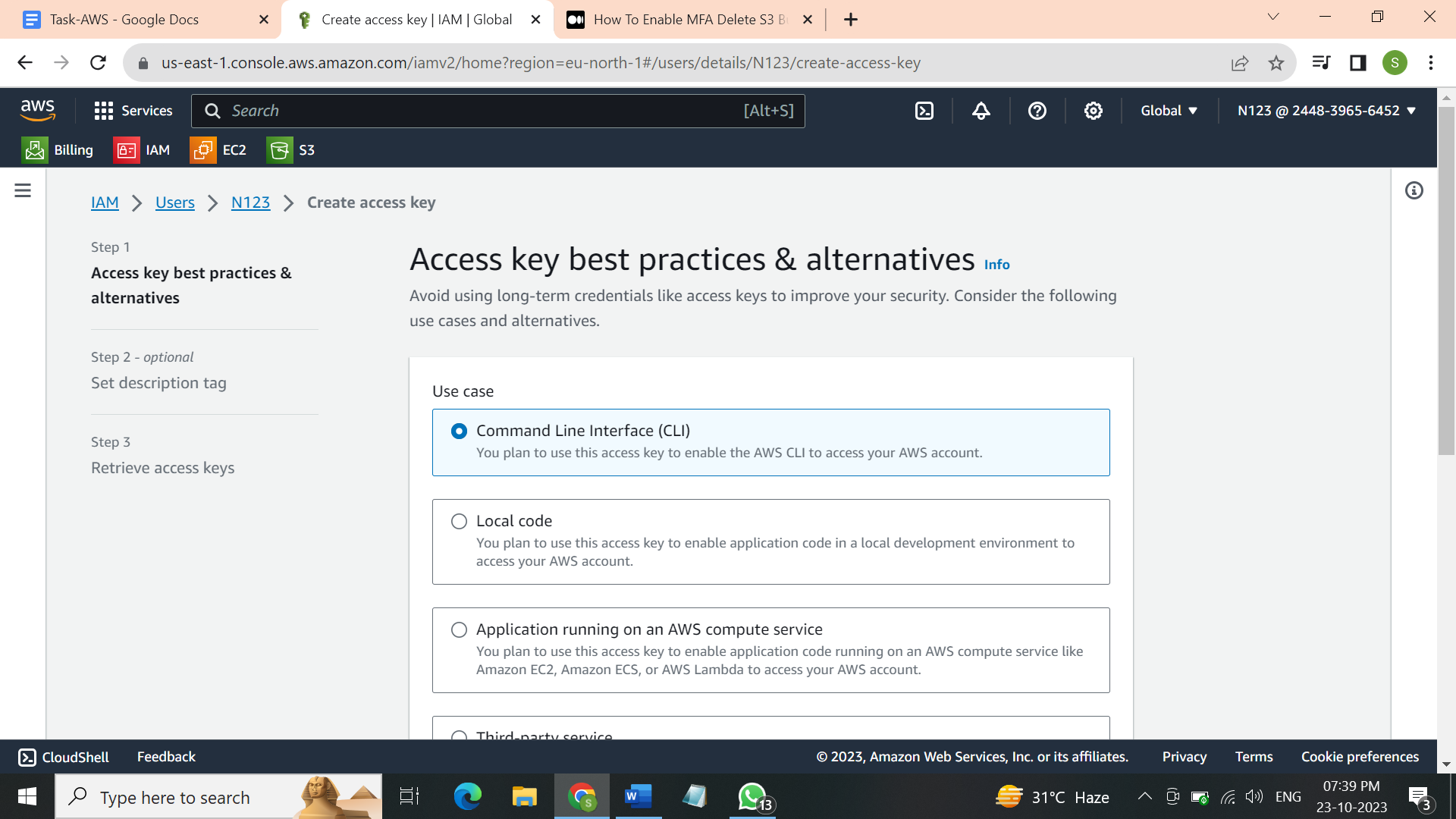
🡪 Step 2 : Upload Object

Enter bucket --- Upload --- drag or browse file --- upload



🡪 Step 3 : Take User Account Keys for CLI access (Create new access key)

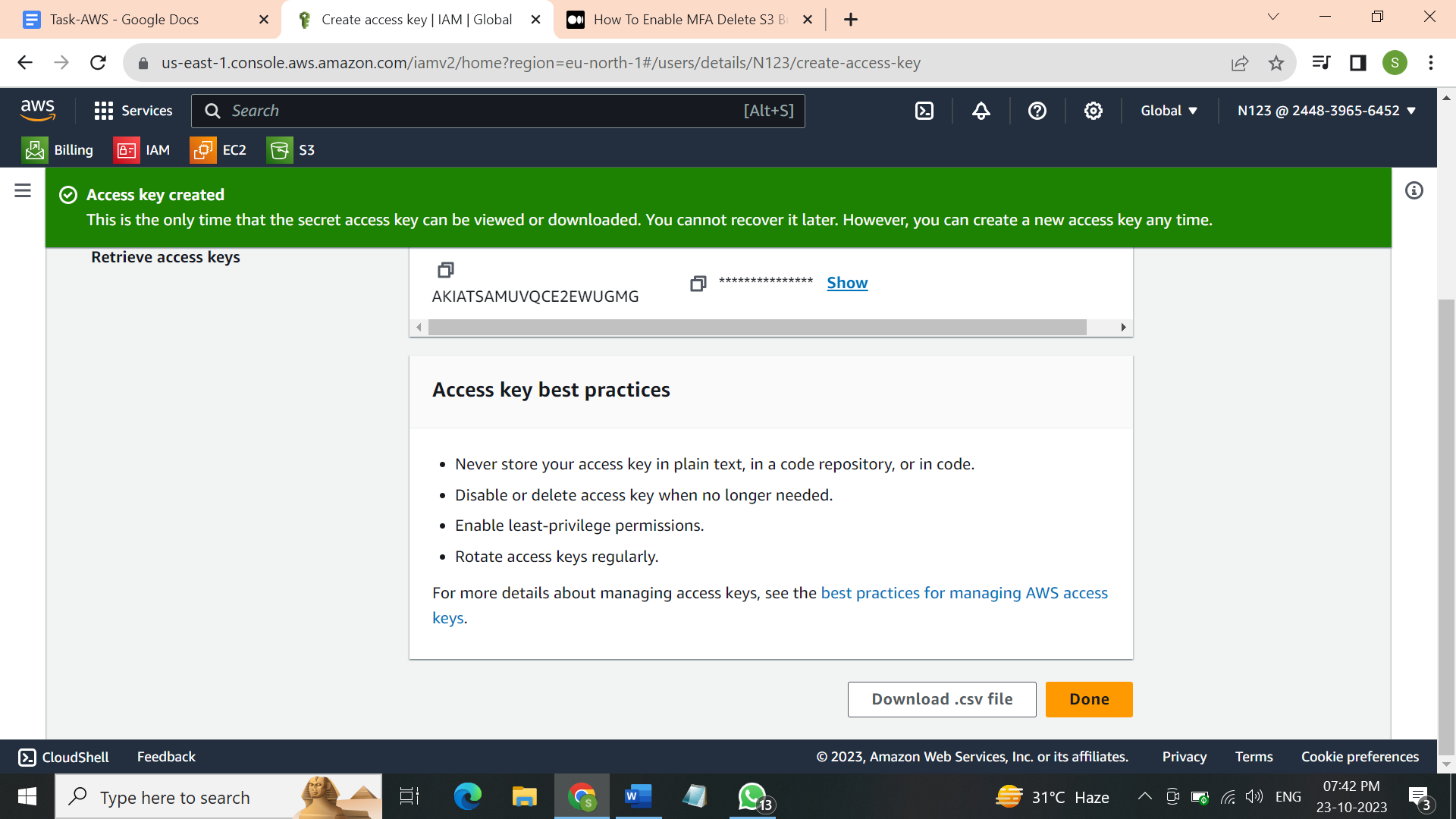
IAM --- Users --- go to particular user --- security credentials --- access keys --- create access key --- select the use case --- command line interface --- next --- give description tag to identify --- next --- download csv file for the access key

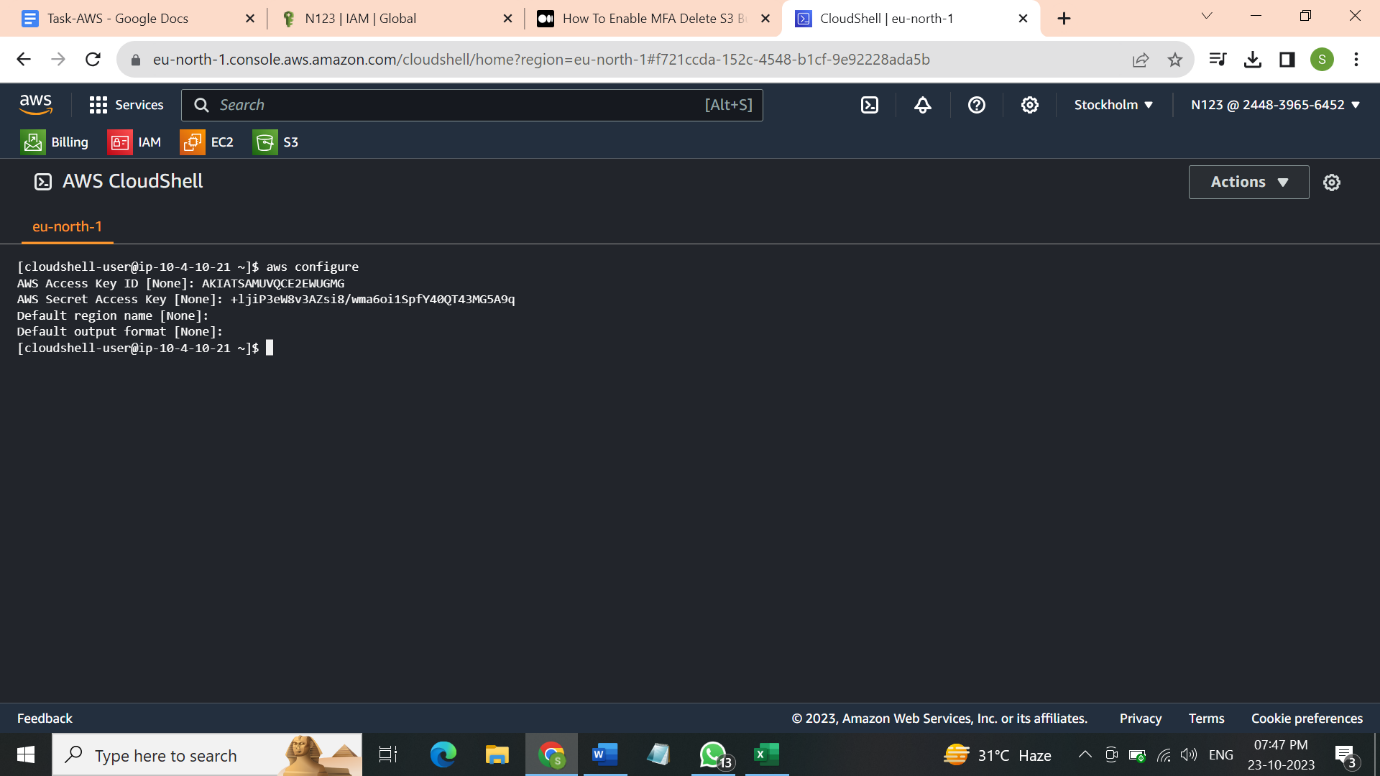
 

Step 4 🡪 Configure AWS CLI with user using access keys ( on cmd prompt or cloudshell)

Cloudshell service --- enter command --- aws configure --- enter access key from csv file ---

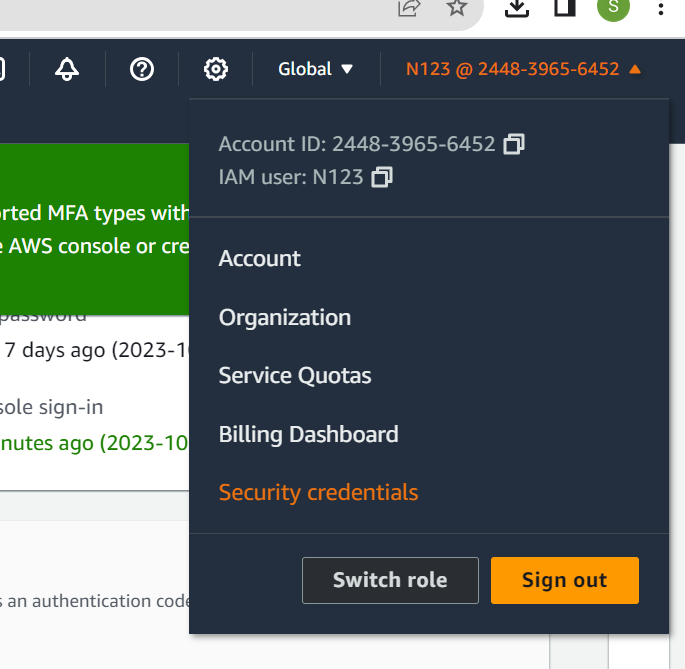
Enter secret access key from csv file --- then check if you can list S3 buckets --- aws s3 ls --- then check if bucket versioning is enabled --- it should be Enabled ---

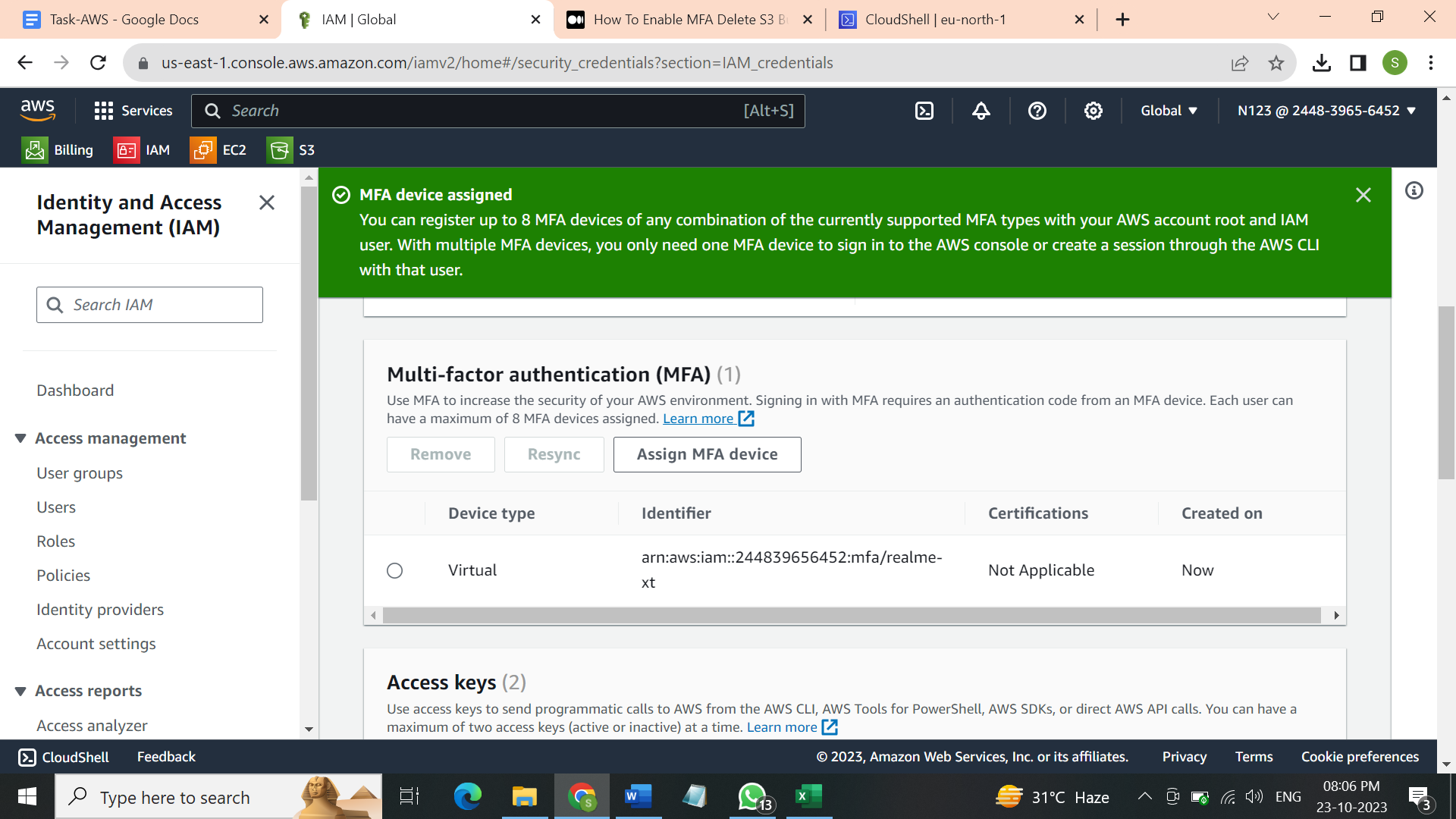




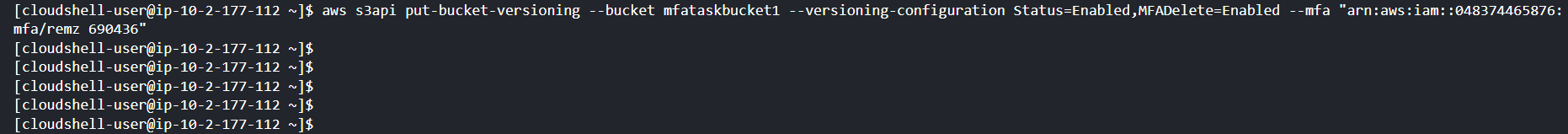
Step 4 🡪 Enable MFA

Download authenticator app and configure all settings





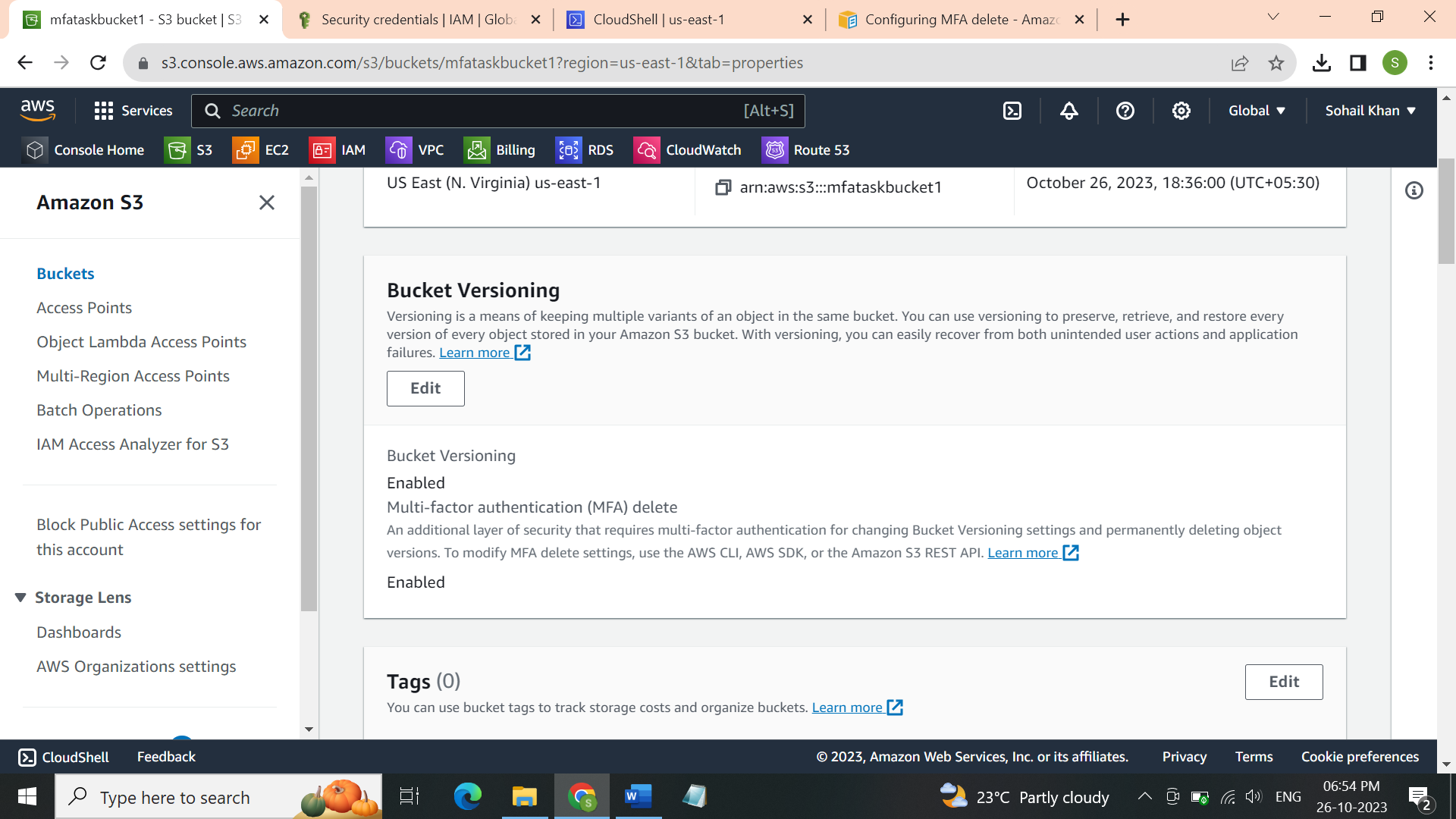
Step 5:- Put command on AWS CLI and then it will be enabled



Command :- aws s3api put-bucket-versioning --bucket (Bucket Name) --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "(MFA Identifier/ARN) (MFA code)"

Example :- aws s3api put-bucket-versioning --bucket mfataskbucket1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::048374465876:mfa/remz 690436"

Step 6: Check bucket’s Properties if MFA Delete is enabled



Step 7 : Now try deleting object from bucket to confirm

Conclusion we can delete the object but we cannot delete its delete marker file and do all this with administrator(root) user account.

