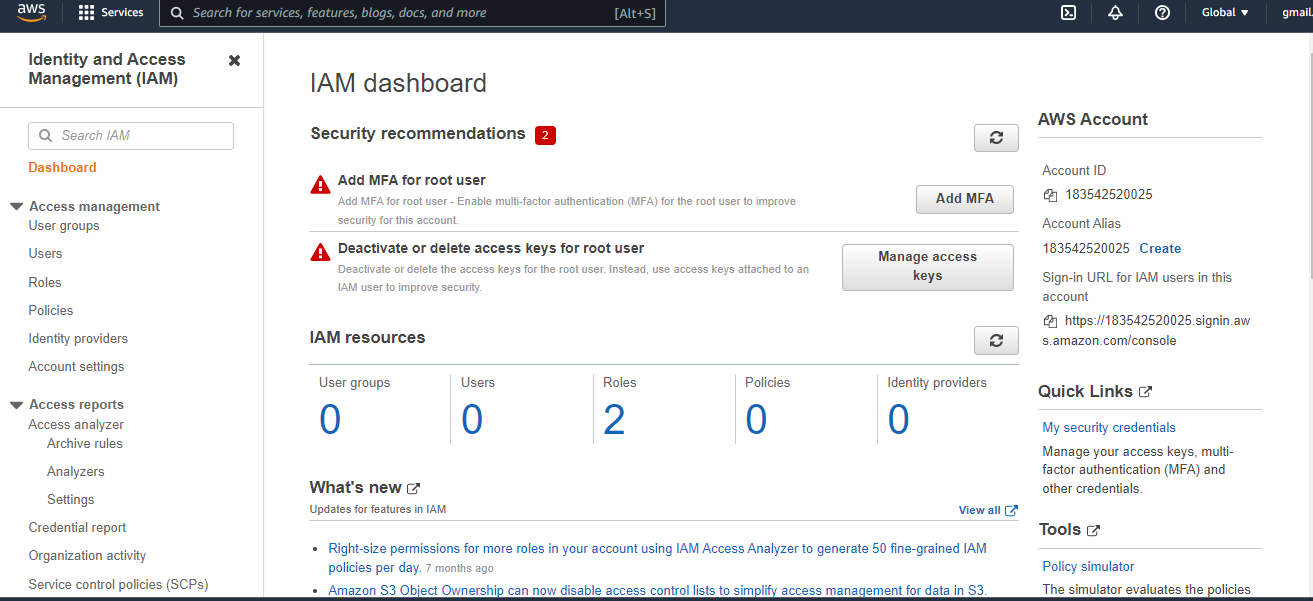
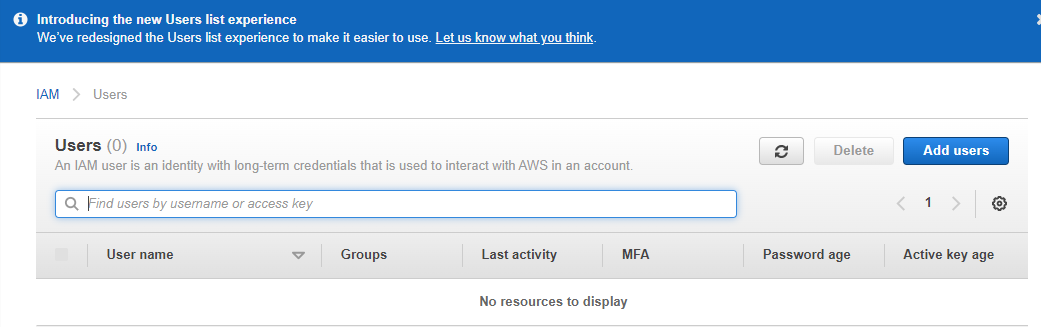
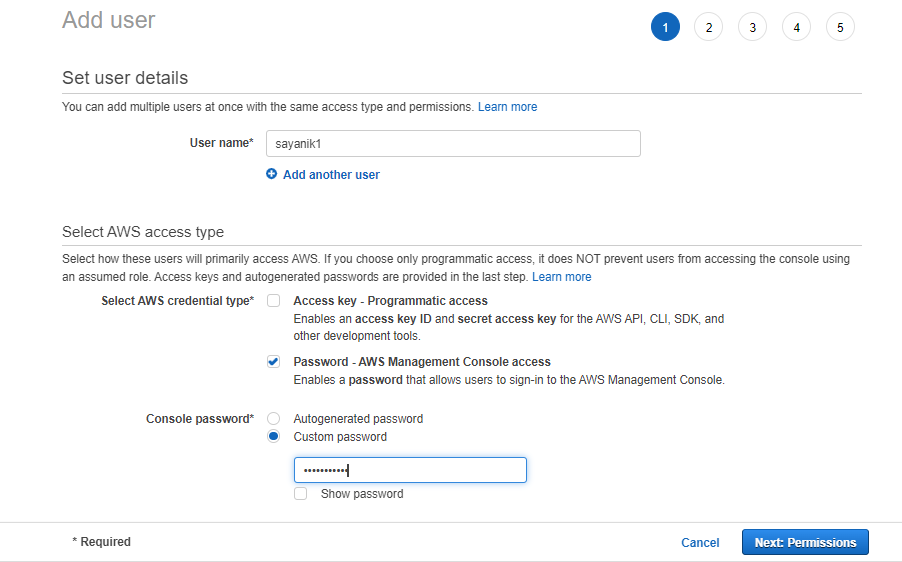
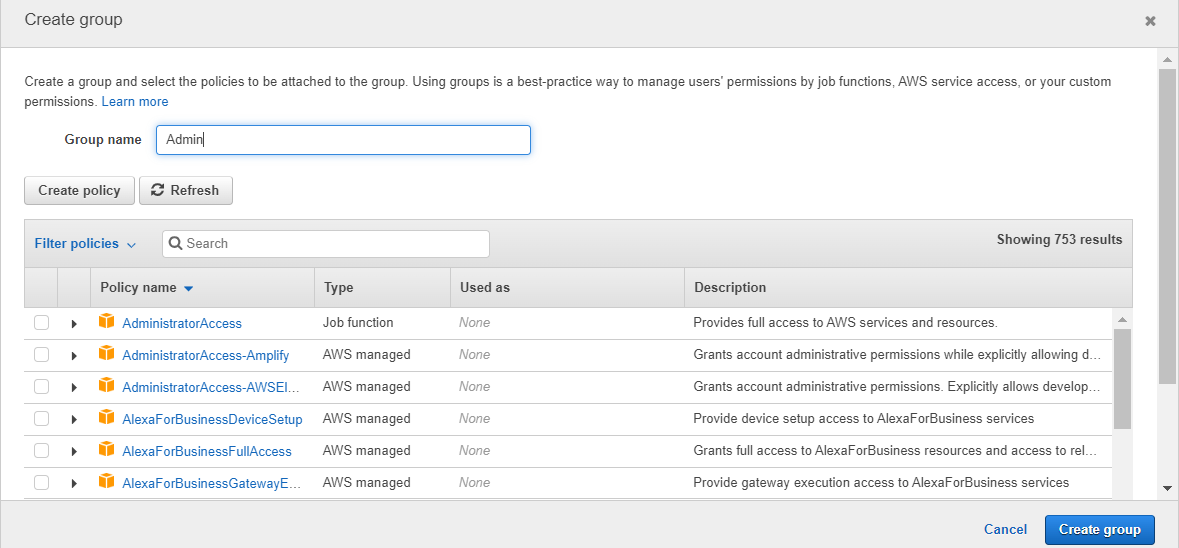
* Create an IAM user.
* Create an ADMIN Group and attach “AdministratorAccess” policies to it. Also provide appropriate tags. Add the user to this group.

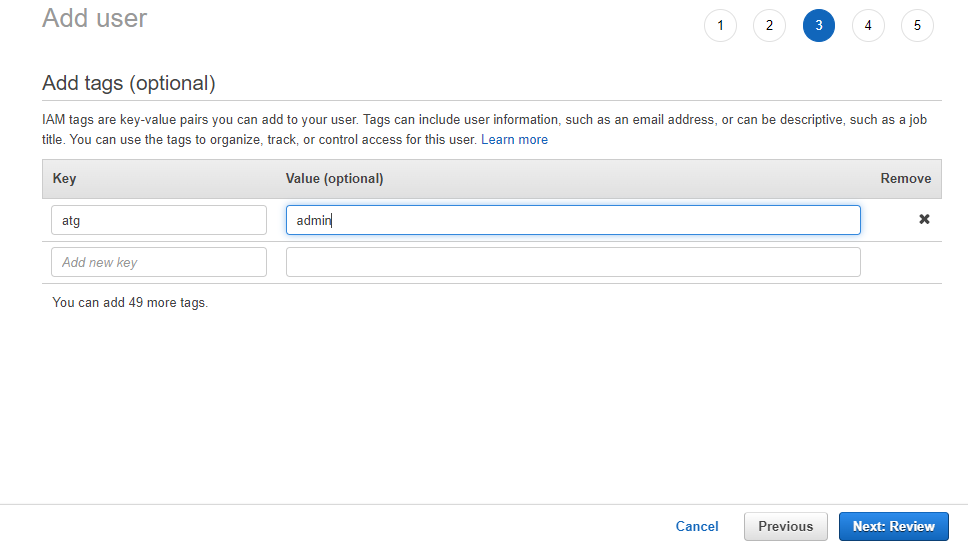
**Note:** When a user is created you need to download the .csv especially if you auto generate a password.

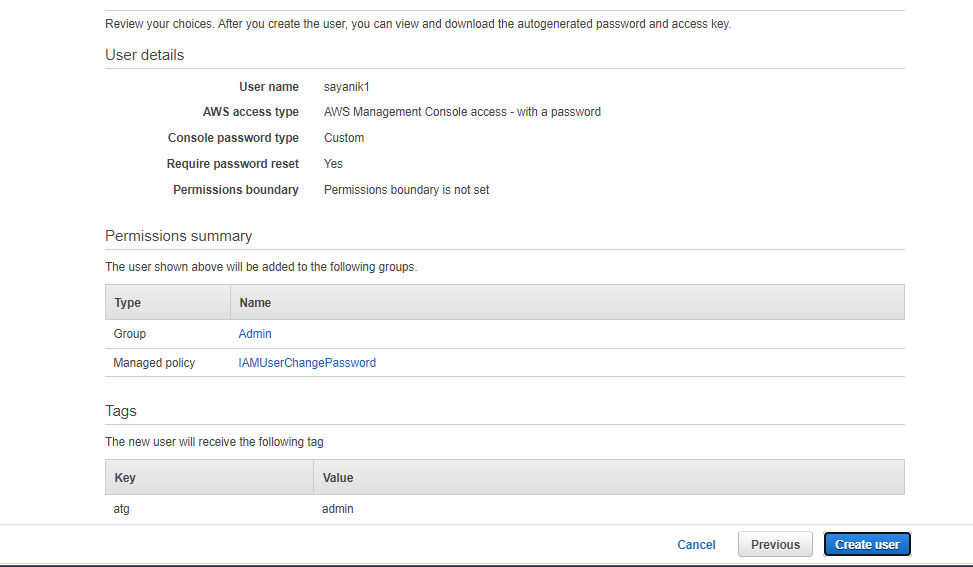


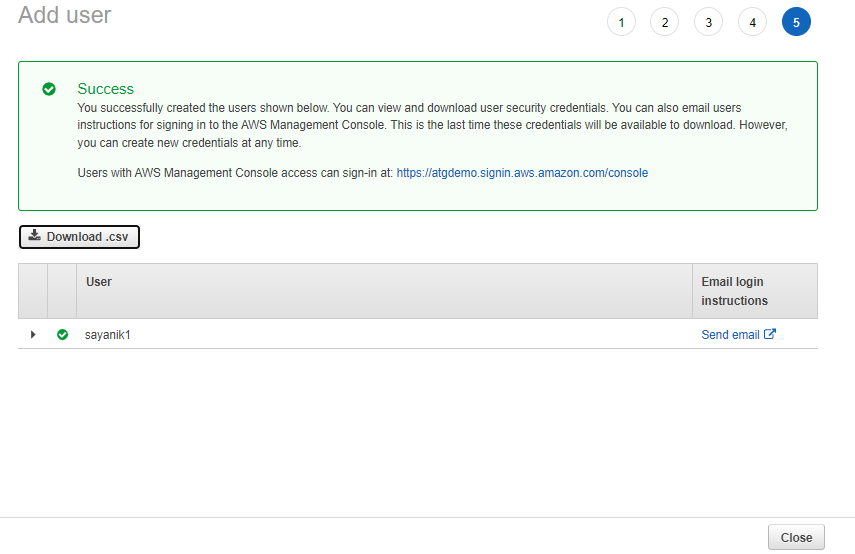


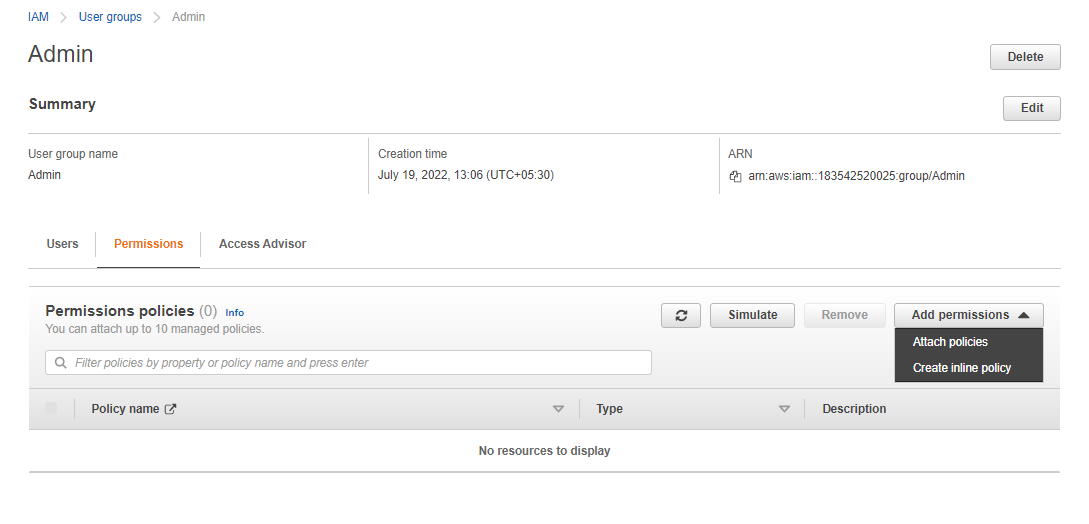


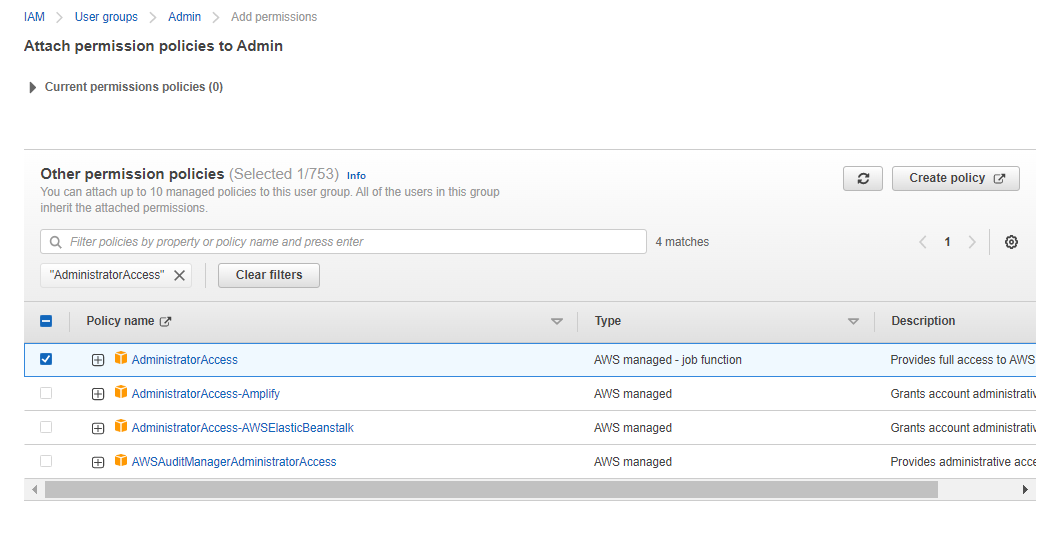


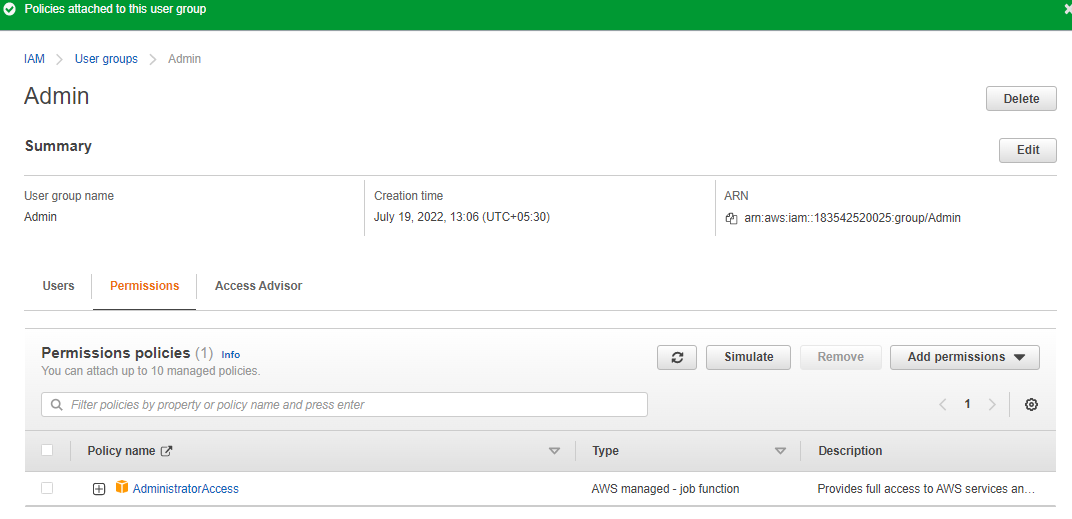


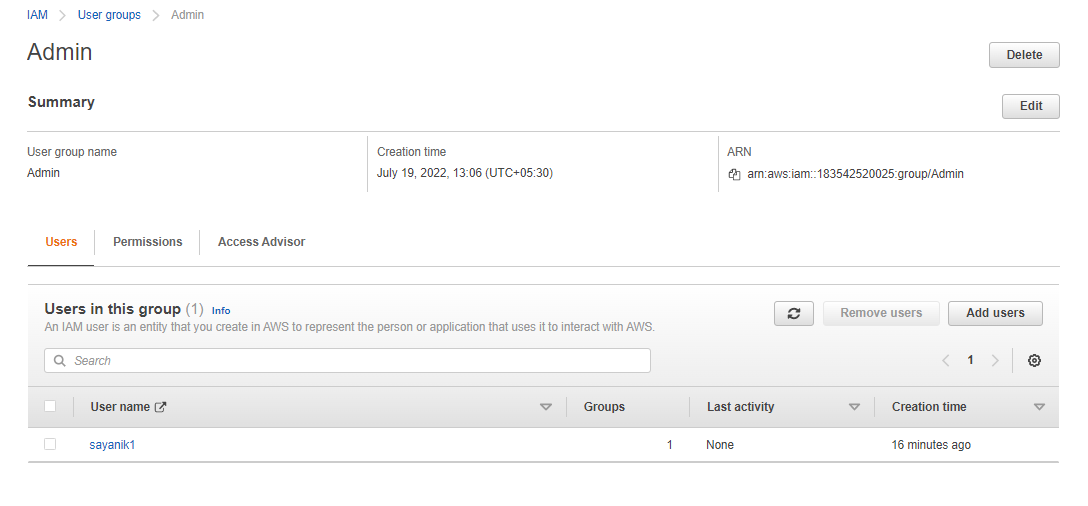




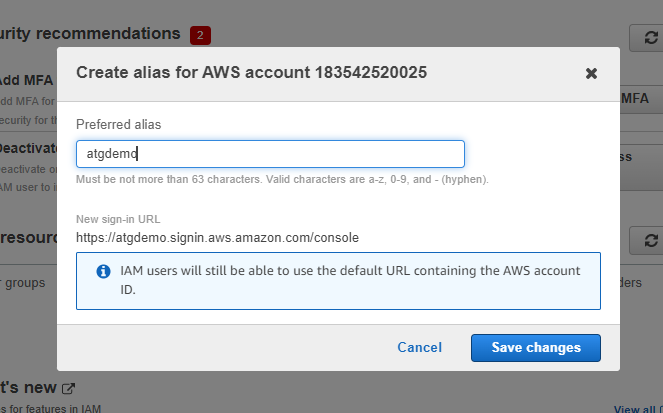


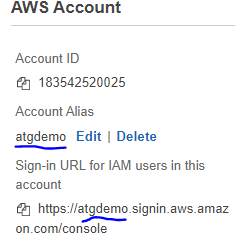


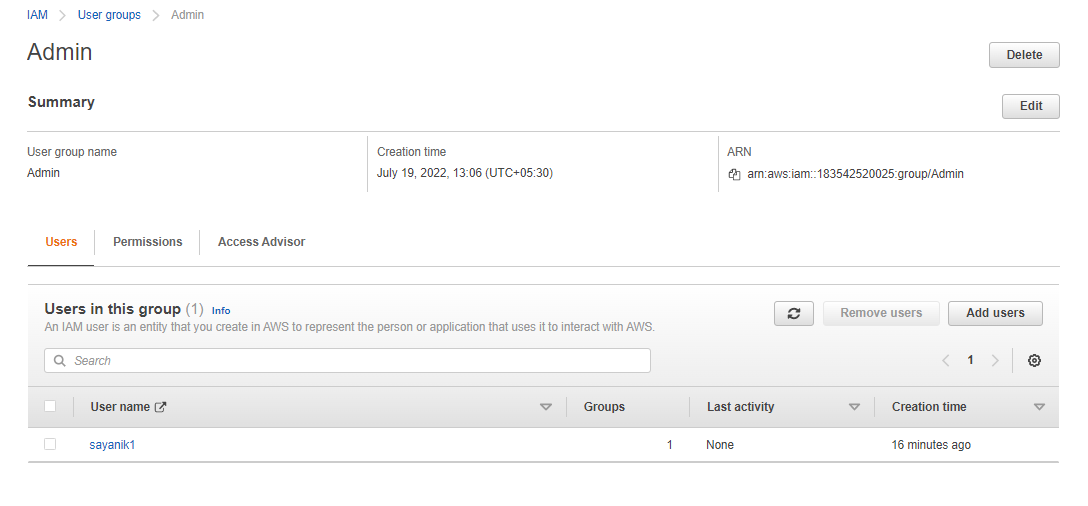


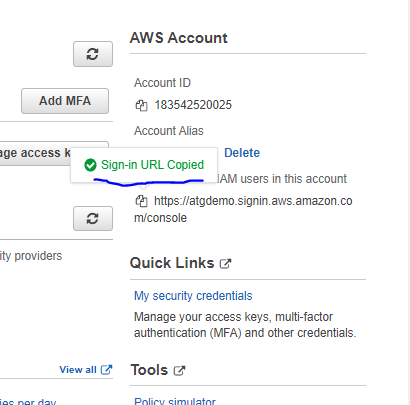


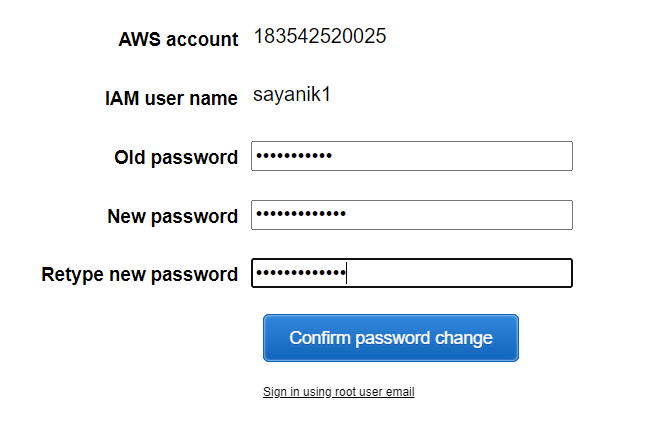
* Create an Account Alias.



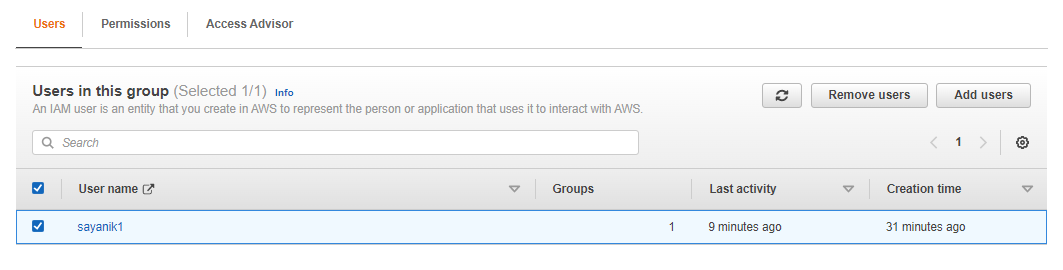


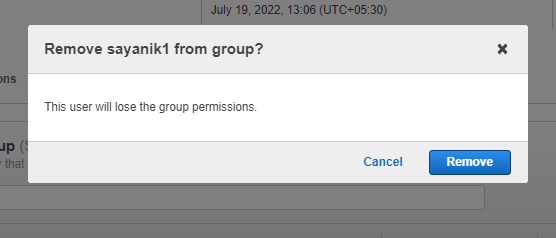


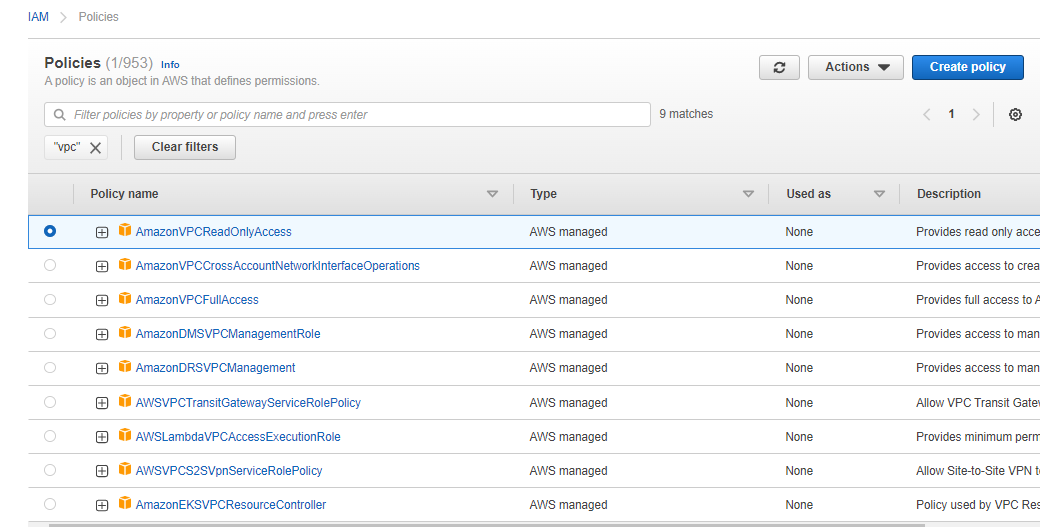


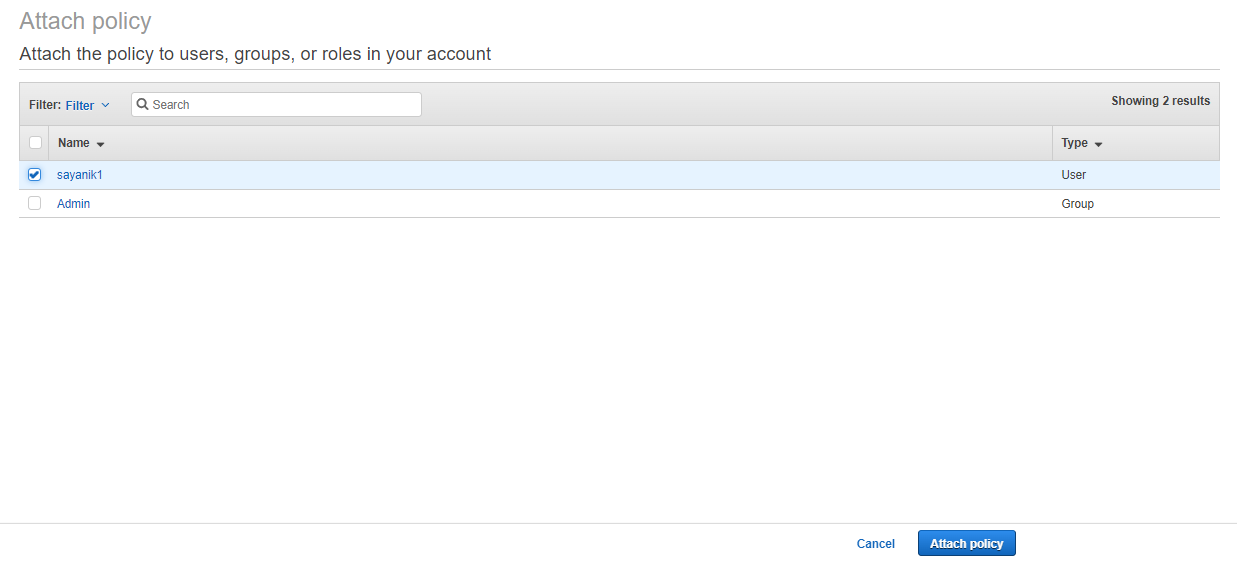


* Remove the user from the admin group.

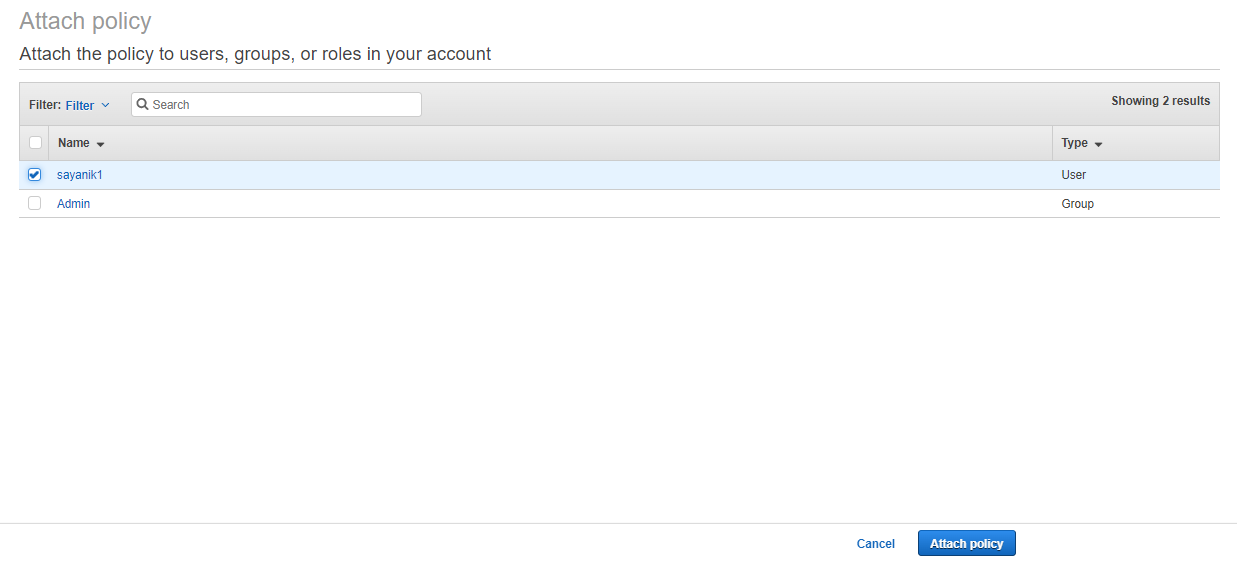


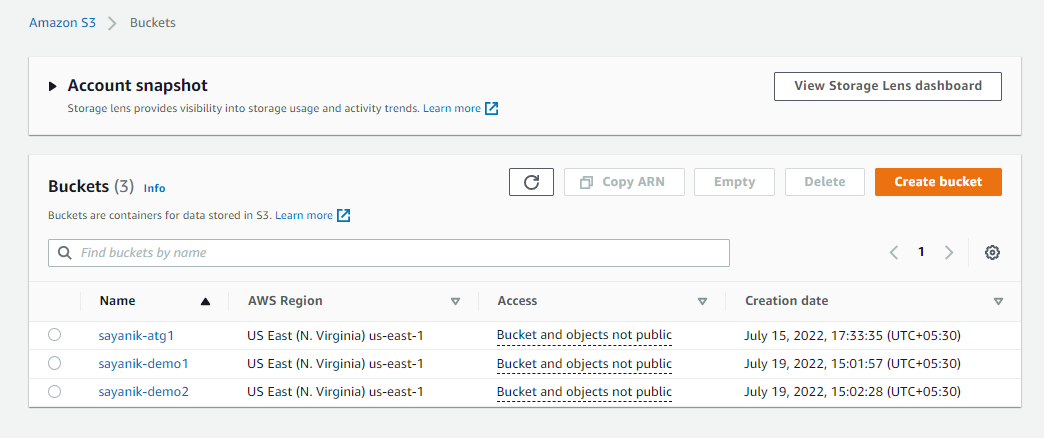


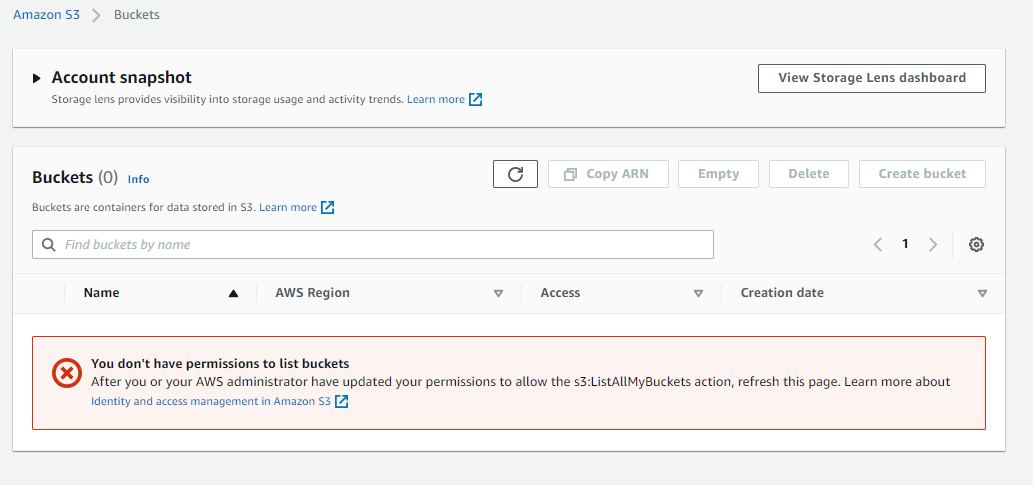


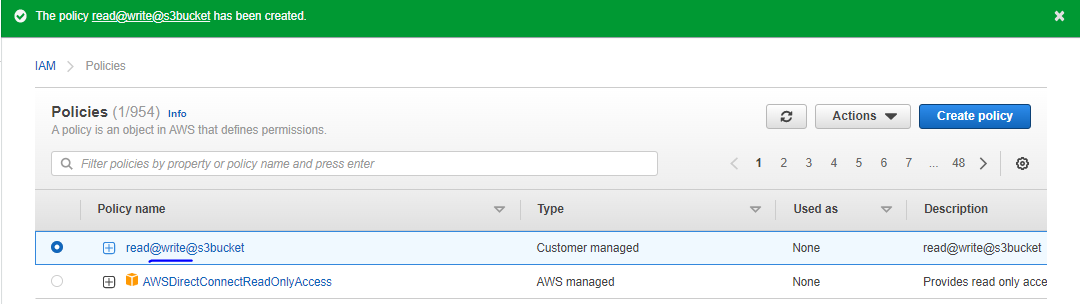


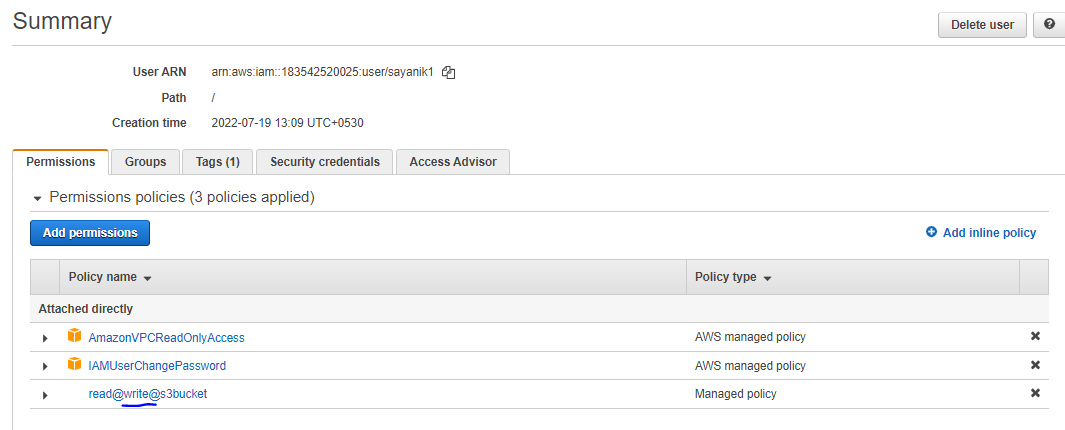
* Add Policies to User using both JSON and inbuilt policies.



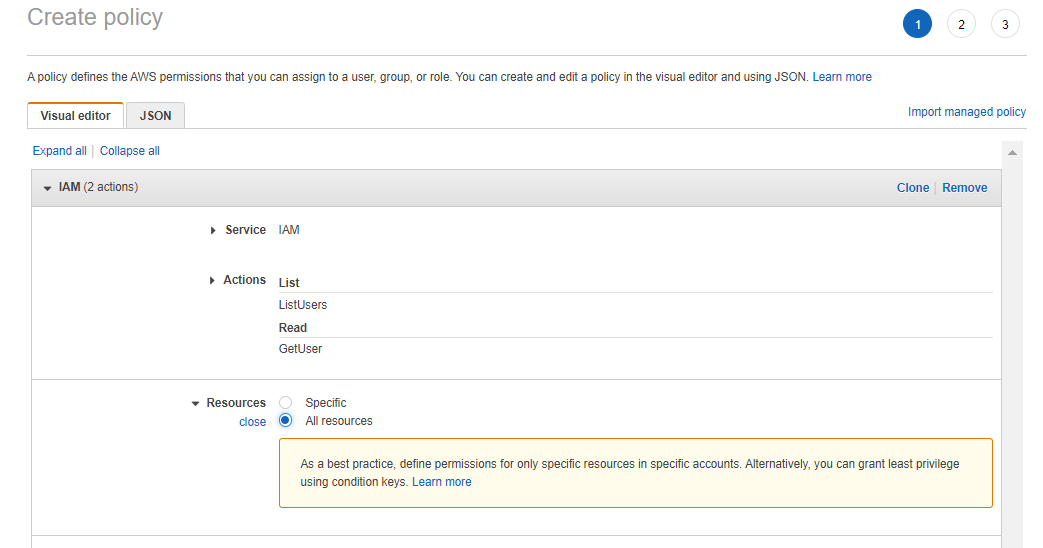


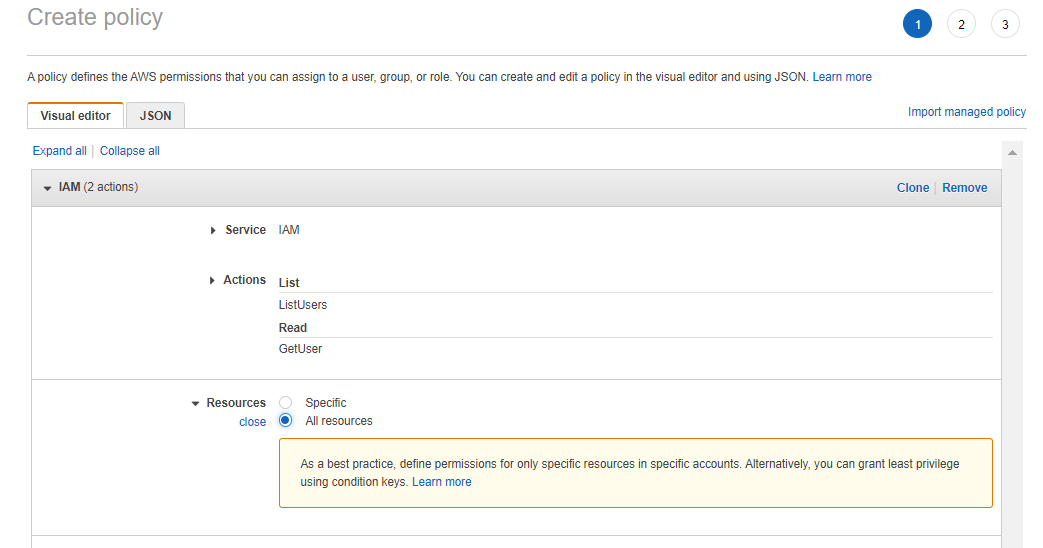


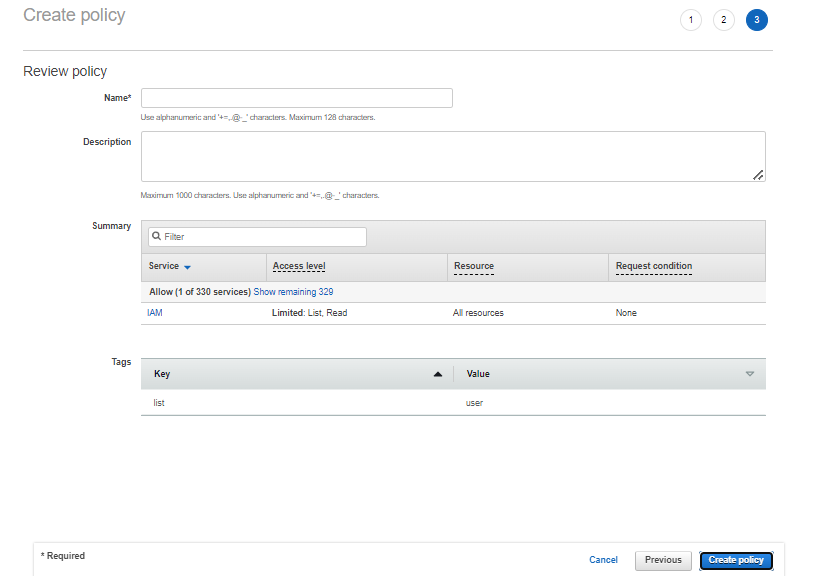


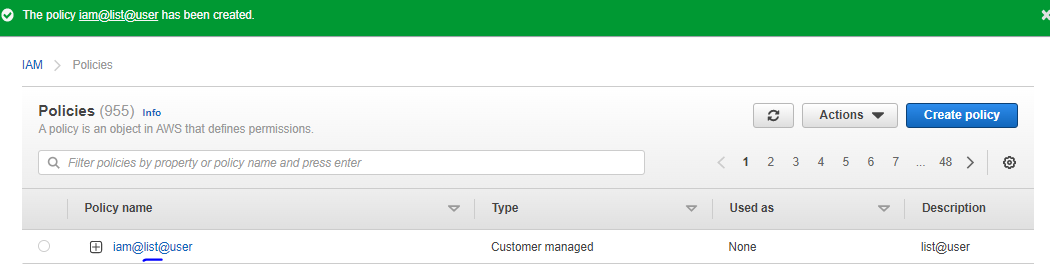


* Create your own policy and attach it to the user.The policy should be of list user.

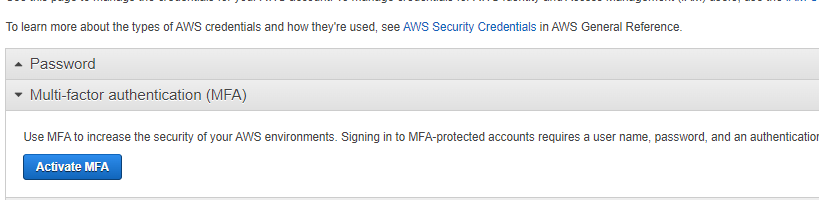


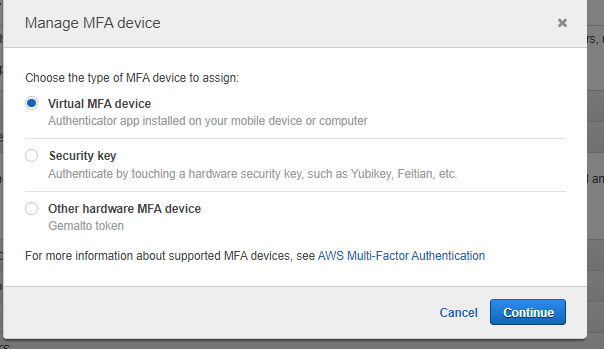


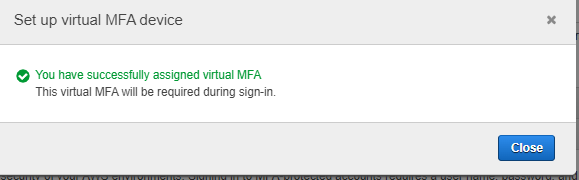




* Create Multi-factor authentication (MFA) in AIM







Create a Role in IAM using AWS EC2 instance with a permissions policy that [grants access to my S3 bucket](https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/)

