





AUTHENTICATION AUTHORIZATION ACCOUNTABILITY

SECURITY

DIGITAL SECURITY

POWERPOINT
FAIRMOMO



ACCOUNTABILITY

Authentication, Authorisation, Accountability



Authentication
- Who you are ?



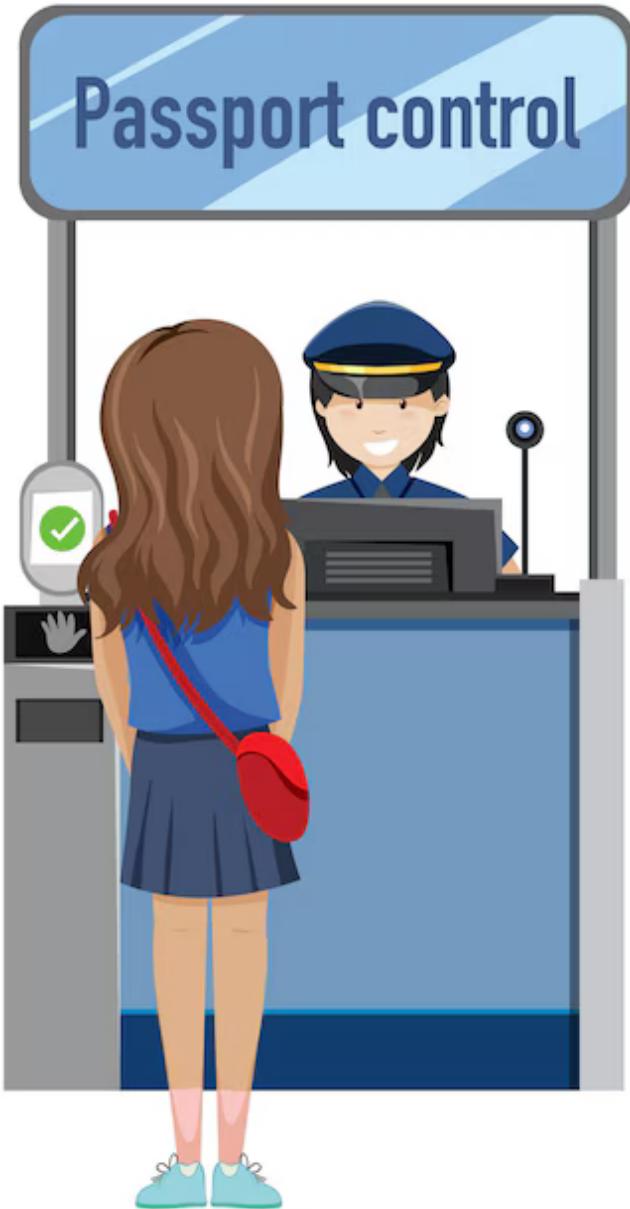
Authorization
- What can you do ?



Accountability
- who did that ?



Authentication, Authorisation, Accountability



Passport



Authentication

- Who you are ?
 - Name:
 - Photo:
 - DOB



Authorization

- What can you do ?
 - Transit
 - Work
 - Tourism

IAM (Identity and Access Management)



AWS IAM

IAM : Identity and Access Management

- ▶ Is a service that helps securely control access to AWS resources.
- ▶ You can use it to manage access to AWS services and resources securely using IAM.
- ▶ You can create and manage AWS users and groups (to support authentication-Who).
- ▶ You can also use IAM for permissions to allow or deny their access to AWS resources (to support authorization-What they can do).

IAM

- ▶ IAM allows you to manage Users, Groups and their level of Access to the AWS Services...



IAM features



IAM user



IAM policy



IAM group



IAM role



Multi-factor authentication

Advantages of IAM

- ▶ Centralized control of your AWS Account
- ▶ Shared access to your AWS Account
- ▶ Granular permissions
- ▶ Identity federation (users can login using LinkedIn , Facebook etc)
- ▶ Multifactor Authentication (password and OTP)
- ▶ Setup password rotation policy (eg: password will expire every 30 days)

Important terms

- ▶ Users - End Users (people)
- ▶ Groups - Collections of users, under one set of permissions.
- ▶ Policies - Set of permissions
- ▶ Roles - We can create roles and assign them to AWS resources

IAM Password Policies

- ▶ Default Password Policy
- ▶ Custom Password Policy



Roles



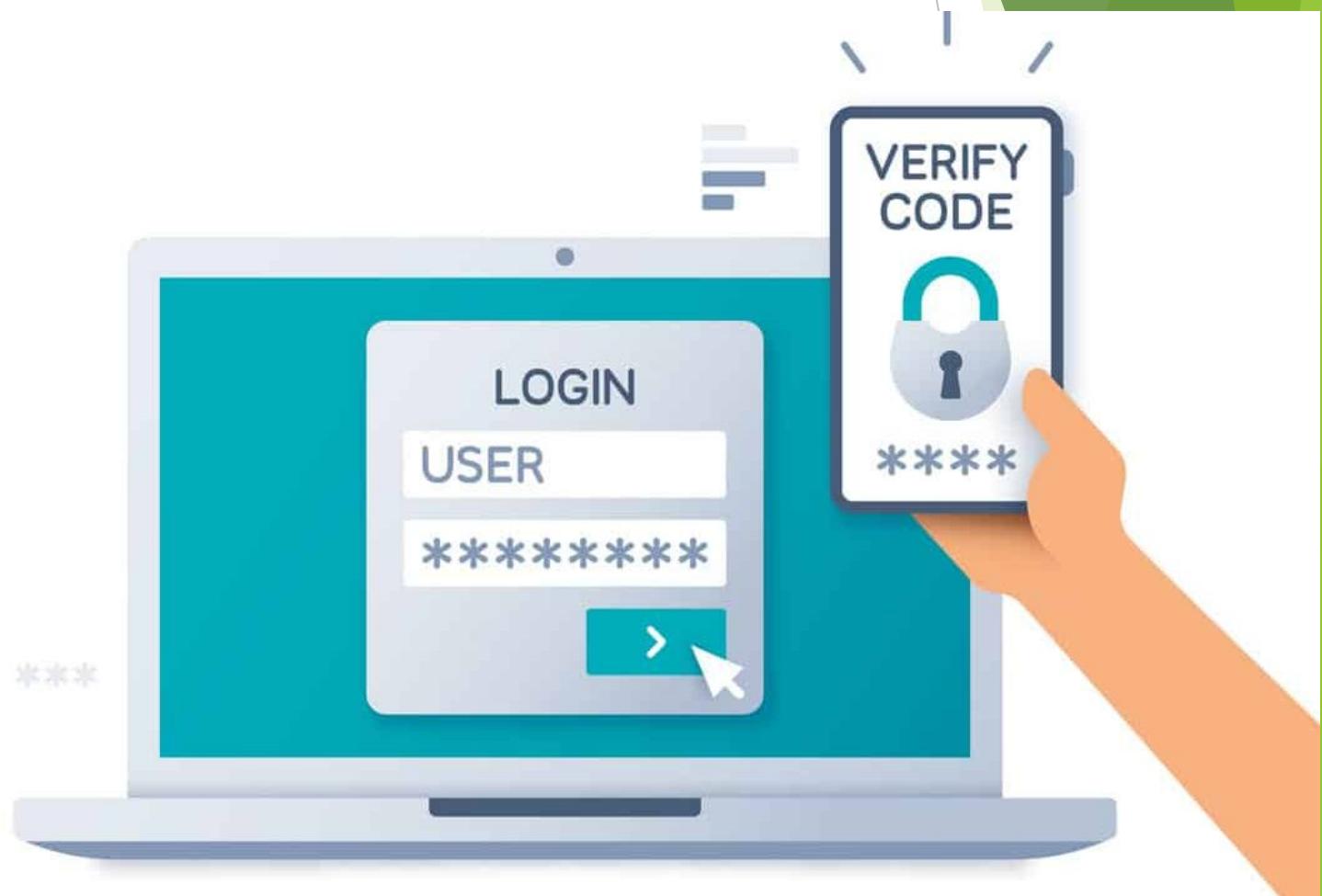
- ▶ Without using credentials, we can manage AWS services through AWS cli by using roles.
- ▶ Roles give secure way to access all AWS resources
- ▶ Can Access one AWS service with another AWS service without credentials.

Important Points

- ▶ IAM is universal. It does not apply to regions at this time.
- ▶ The “root account” is simply the account created when first setup your AWS account. It has complete Admin access.
- ▶ New Users have NO permissions when first created.
- ▶ New Users are assigned Access Key ID & Secret Access Key ID & Secret Access Keys when first created.
- ▶ These are not the same as a password, and you cannot use the Access key ID & Secret Access key to login in to the console. You can use this to access command line.
- ▶ You can create and customize your own password rotation policies.

IAM user - Security Credentials

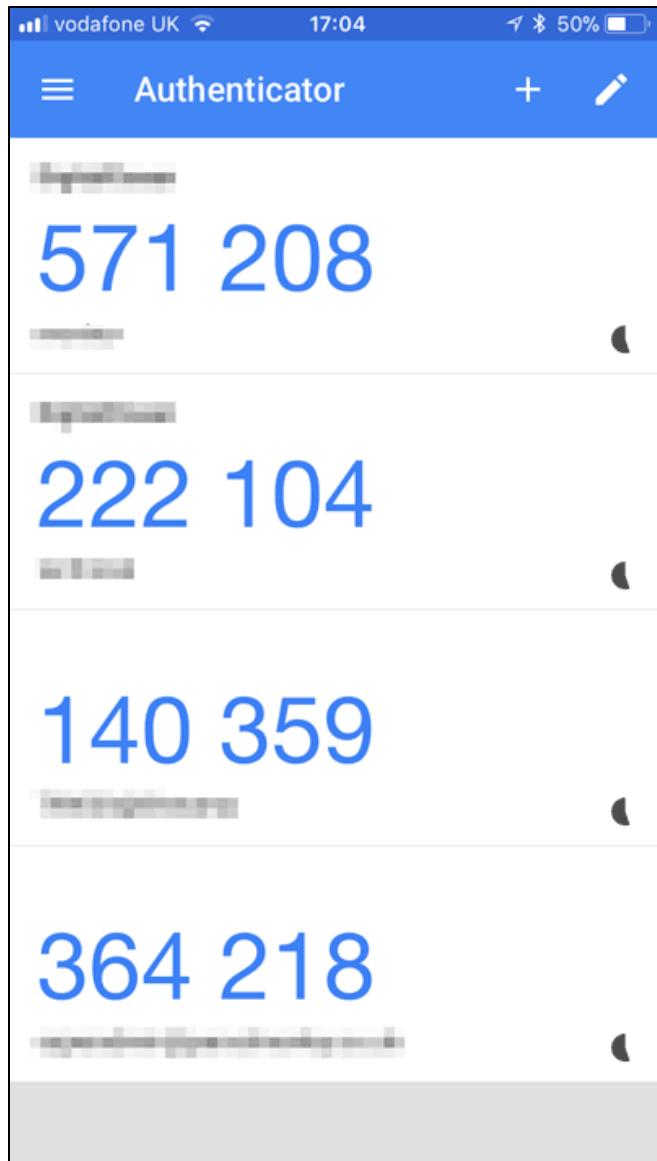
- ▶ Console sing-in
- ▶ Multi-factor authentication (MFA)
- ▶ Access key & Sec Access key



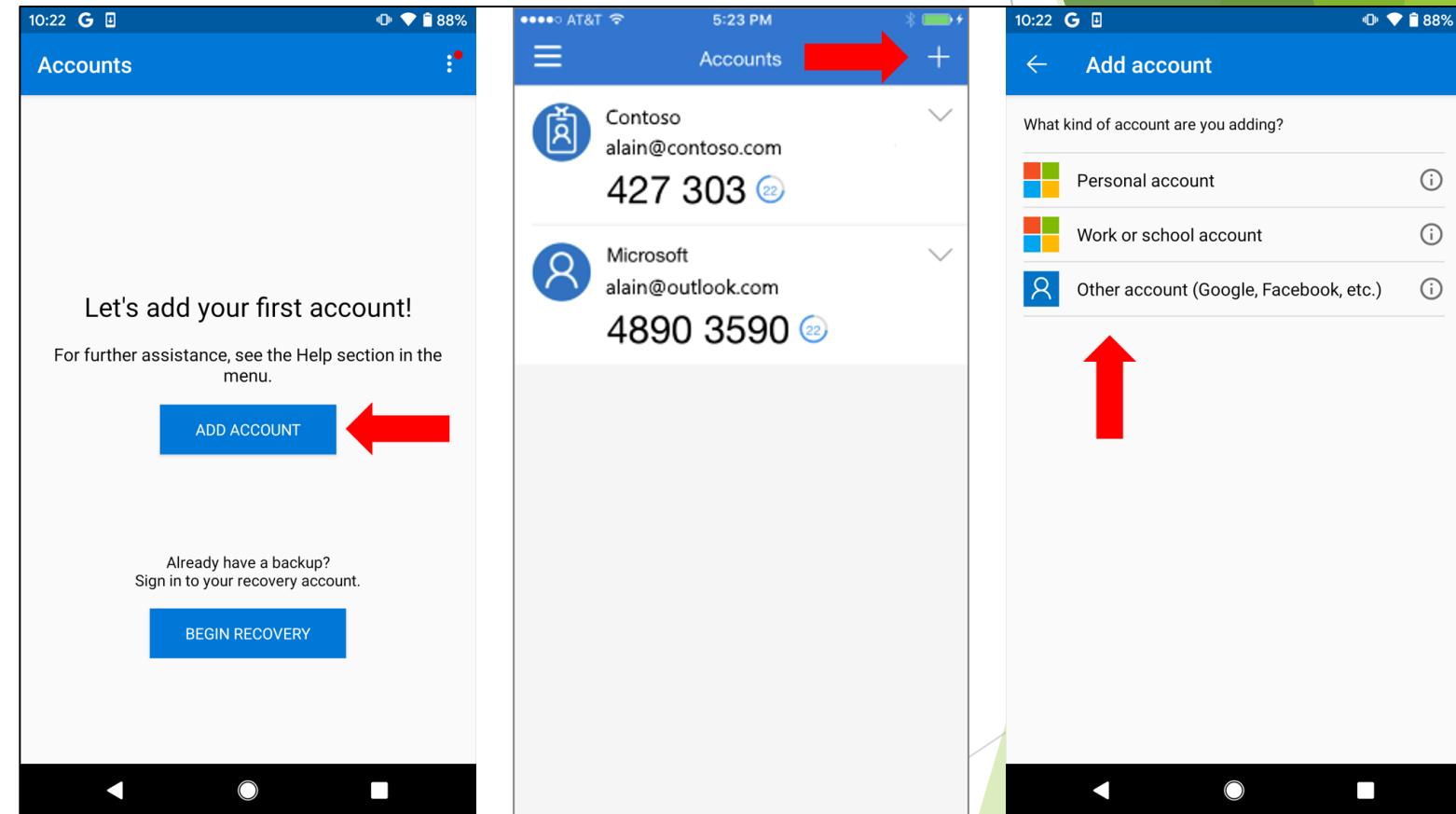
What is Multi-Factor authentication (MFA)

- ▶ Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint. A second form of authentication can help prevent unauthorized account access if a system password has been compromised.

Google Authenticator



Microsoft Authenticator



Type of security credentials

Type of credentials	Association
Email address and password	Associated with an AWS account (root)
IAM user name and password	Used for accessing the AWS Management Console
Access and secret access key	Typically used with the AWS command line interface (AWS CLI) and programmatic requests, such as application programming interfaces (APIs) and software development kits (SDKs)
Multi-factor authentication (MFA)	Used to provide as an extra layer of security, which can be enabled for AWS account root user and IAM users
Key pairs	Used for only specific AWS services, such as Amazon EC2

How to connect with AWS CLI

- ▶ Download CLI form Amazon website for your server.
- ▶ <https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

- ▶ #aws configure
- ▶ #aws iam list-users
- ▶ #aws iam list-groups
- ▶ #aws iam create-user --user-name jerry
- ▶ #aws iam create-group --group-name marketing
- ▶ #

How to connect with AWS CLI

- ▶ #aws s3 ls
- ▶ #aws s3 mb s3://123abcd (create Bucket)
- ▶ #aws s3 rb s3://“Bucket name” (delete bucket)
- ▶ #aws s3 sync . S3://“bucket name” (sync folder data from s3 to local) Upload
- ▶ #aws s3 sync s3://“Bucket name” . (sync s3 data to local)