What Is IAM?

**Identity and Access Management (IAM)** is where you manage your AWS users, groups, and roles, as well as their access to AWS accounts and services:

* IAM provides access and access permissions to AWS resources (such as EC2, S3 and DynamoDB)
* IAM is global to all AWS regions — creating a user account will apply to all regions

When you first create an AWS account, it is a root user account.

According to best practices, it is strongly recommended not to use the root user and create another user with administrative permissions for yourself.

By default, any new IAM user you create in an AWS account (not a root user) is created with no access to any AWS services. This is a **non-explicit deny** rule set on all new IAM users.

Best practices:

* it is strongly recommended not to use the root user and create another user with administrative permissions for yourself
* when a new AWS root account is created, complete the tasks listed in IAM under Security Status

1. *Delete your root access keys*
2. *Activate MFA on your root account*
3. *Create individual IAM users*
4. *User IAM groups to assign permissions*
5. *Apply an IAM password policy*

* always follow the **principle of least privilege** when administering AWS accounts, users, groups and roles

## IAM Features

IAM gives you the following features:

* **Shared access to your AWS account**

You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

* **Granular permissions**   
  You can grant different permissions to different people for different resources. (for example, you might allow some users complete access to EC2, S3 and for other user you can allow read-only access)
* **Secure access to AWS resources for applications that run on Amazon EC2**   
  You can use IAM features to securely provide credentials for applications that run on EC2 instances. These credentials provide permissions for your application to access other AWS resources. (for example, S3 buckets)
* **Multi-factor authentication (MFA)** You can add two-factor authentication to your account and to individual users for extra security.
* **Identity federation** You can allow users to get temporary access to your AWS account, if they are not granted with some permissions
* **Identity information for assurance**If you use AWS CloudTrail, you receive log records that include information about those who made requests for resources in your account. That information is based on IAM identities.

## Accessing IAM

* **AWS Management Console**The console is a browser-based interface to manage IAM and AWS resources.
* **AWS Command Line Tools**You can use the AWS command line tools to issue commands at your system's command line to perform IAM and AWS tasks (AWS CLI).
* **AWS SDKs**  
   AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms.
* **IAM HTTPS API**   
  You can access IAM and AWS programmatically by using the IAM HTTPS API, which lets you issue HTTPS requests directly to the service.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>