How IAM Works

The IAM infrastructure includes the following elements:

* **Terms**
* **Principal**
* **Request**
* **Authentication**
* **Authorization**
* **Actions or Operations**
* **Resources**

Terms

* **Resources**   
  The user, group, role, policy, and identity provider objects that are stored in IAM.
* **Identities**   
  The IAM resource objects that are used to identify and group — users, groups and roles.
* **Entities**   
  The IAM resource objects that AWS uses for authentication — users and roles
* **Principals**   
   A person or application that uses the AWS account root user, an IAM user/role to sign in and make requests to AWS.

Principal

A **principal**is a person or application that can make a request for an action or operation on an AWS resource.

The principal is authenticated as the AWS account root user or an IAM entity to make requests to AWS. As a best practice, do not use your root user credentials for your daily work. Instead, create IAM entities.

Request

When a principal tries to use the AWS Management Console, the AWS API, or the AWS CLI, that principal sends a **request** to AWS.

The request includes the following information:

* **Actions or operations**   
   The actions or operations that the principal wants to perform.
* **Resources** The AWS resource object upon which the actions or operations are performed.
* **Principal**   
   The person or application that used an entity (user or role) to send the request.
* **Environment data**  
  Information about the IP address, user agent, SSL enabled status, or the time of day.
* **Resource data**  
   Data related to the resource that is being requested.

Authentication

A principal must be authenticated (signed in to AWS) using their credentials to send a request to AWS.

## Authorization

You must also be authorized (allowed) to complete your request.

During authorization, AWS uses values from the request context to check for policies. It then uses the policies to determine whether to allow or deny the request. Most policies are stored in AWS as JSON documents and specify the permissions for principal entities.

By default, all requests are denied, AWS authorizes your request only if every part of your request is allowed. (In general, requests made using the AWS account root user credentials for resources in the account are always allowed.)

AWS checks each policy that applies to the context of your request. If a single permissions policy includes a denied action, AWS denies the entire request and stops evaluating. This is called an **explicit deny**.

## Actions or Operations

After your request has been authenticated and authorized, AWS approves the actions or operations in your request. Operations are defined by a service, and include things that you can do to a resource, such as viewing, creating, editing, and deleting that resource.

Resources

The service defines a set of actions that can be performed on each resource. If you create a request to perform an unrelated action on a resource, that request is denied.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html>

<https://docs.aws.amazon.com/IAM/latest/UserGuide/images/intro-diagram%20_policies_800.png>