**IAM Users**

**User**is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

## How AWS identifies an IAM user

When you create a user, IAM creates these ways to identify that user:

* **A "friendly name" for the user**   
   The name that you specified when you created the user (such as Richard or Anaya). These are the names you see in the AWS Management Console.
* **An Amazon Resource Name (ARN) for the user**   
  You use the ARN when you need to uniquely identify the user across all of AWS. (*arn:aws:iam::account-ID-without-hyphens:user/Richard*)
* **A unique identifier for the user**   
   This ID is returned only when you use the API, Tools for Windows PowerShell, or AWS CLI to create the user; you do not see this ID in the console.

IAM ARNs

*Amazon Resource Name (ARN)* format:

arn:*partition*:*service*:*region*:*account*:*resource*

Where:

* **partition** - identifies the partition that the resource is in (for standard AWS regions, the partiotion is ***aws***)
* **service** — identifies the AWS product (for example, ***iam***)
* **region** - is the Region the resource resides in
* **account** — is the AWS account ID with no hyphens (for example, ***123456789***)
* **resource** - is the portion that identifies the specific resource by name

## 

## 

## 

## Users and credentials

IAM users receive unique credentials so you should not share with others.

You can access AWS in different ways depending on the user credentials:

* **Console password**A password that the user can type to sign in to interactive sessions such as the AWS Management Console.
* **Access keys**   
   A combination of an access key ID and a secret access key. You can assign two to a user at a time. (For example, you might use access keys when using the API for code or at a command prompt when using the AWS CLI or the AWS PowerShell tools)
* [**SSH keys for use with CodeCommit**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_ssh-keys.html)   
   An SSH public key in the OpenSSH format that can be used to authenticate with CodeCommit.
* **Server certificates**   
   SSL/TLS certificates that you can use to authenticate with some AWS services.

By default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. You must create the type of credentials for an IAM user based on the needs of your user.

* [**Manage passwords for your IAM users**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords.html)  
   Create and change the passwords that permit access to the AWS Management Console. Set a password policy to enforce a minimum password complexity. Allow users to change their own passwords.
* [**Manage access keys for your IAM users**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) Create and update access keys for programmatic access to the resources in your account.
* **Enable** [**multi-factor authentication (MFA)**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html)  
   With MFA, users have to provide two forms of identification: First, they provide the credentials that are part of their user identity (a password or access key). In addition, they provide a temporary numeric code that's generated on a hardware device or by an application on a smartphone or tablet, or sent by AWS to an SMS-compatible mobile device.
* [**Find unused passwords and access keys**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_finding-unused.html)   
   Anyone who has a password or access keys for your account or an IAM user in your account has access to your AWS resources. The security [best practice](https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html)is to remove passwords and access keys when users no longer need them.
* [**Download a credential report for your account**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html)   
  You can generate and download a credential report that lists all IAM users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. For passwords and access keys, the credential report shows how recently the password or access key has been used.

Users and policies

When first created, by default an IAM user has a **non-explicit «deny»** for AWS services and does not have access to them until a policy granting allow access has been applied to the user or to the group the user belongs to.

By default, a brand new IAM user has no [permissions](https://docs.aws.amazon.com/IAM/latest/UserGuide/access.html) to do anything. The user is not authorized to perform any AWS operations or to access any AWS resources. An advantage of having individual IAM users is that you can assign permissions individually to each user.

You can also add a permissions boundary to your users. A permissions boundary is an advanced feature that allows you to use AWS managed policies to limit the maximum permissions that an identity-based policy can grant to a user or role.

## Users and accounts

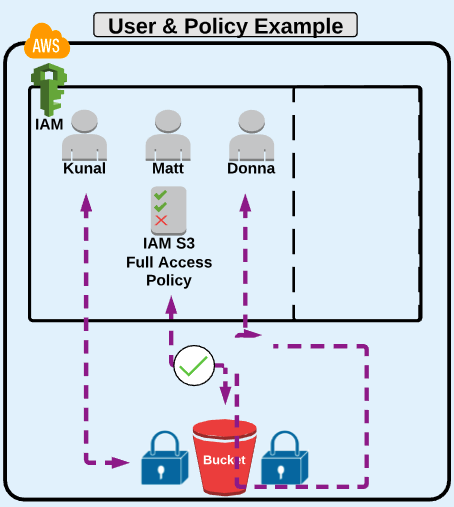
Each IAM user is associated with one and only one AWS account. Because users are defined within your AWS account, they don't need to have a payment method on file with AWS. Any AWS activity performed by users in your account is billed to your account.

There's a limit to the number of IAM users you can have in an AWS account.

## Users as service accounts

An IAM user is a resource in IAM that has associated credentials and permissions. An IAM user can represent a person or an application that uses its credentials to make AWS requests. This is typically referred to as a **service account**.

If you choose to use the long-term credentials of an IAM user in your application, **do not embed access keys directly into your application code.** The AWS SDKs and the AWS Command Line Interface allow you to put access keys in known locations so that you do not have to keep them in code.



<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_identity-management.html>

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