Create an IAM user in your AWS account

Archived: 2026-04-05 23:18:16 UTC

1.
2.
3.

4. User Guide

Focus mode

Important

IAM best practices recommend that you require human users to use federation with an identity provider to access AWS using temporary credentials instead of using IAM users with long-term credentials. We recommend that you only use IAM users for specific use cases not supported by federated users.

The process of creating an IAM user and enabling that user to perform tasks consists of the following steps:

1. Create the user in the AWS Management Console, the AWS CLI, Tools for Windows PowerShell, or using an AWS API operation. If you create the user in the AWS Management Console, then steps 1–4 are handled automatically, based on your choices. If you create the IAM users programmatically, then you must perform each of those steps individually.

2. Create credentials for the user, depending on the type of access the user requires:

   - **Enable console access – *optional***: If the user needs to access the AWS Management Console, create a password for the user. Disabling console access for a user prevents them from signing in to the AWS Management Console using their user name and password. It does not change their permissions or prevent them from accessing the console using an assumed role.

   Tip

   Create only the credentials that the user needs. For example, for a user who requires access only through the AWS Management Console, do not create access keys.

3. Give the user permissions to perform the required tasks. We recommend that you put your IAM users in groups and manage permissions through policies that are attached to those groups. However, you can also grant permissions by attaching permissions policies directly to the user. If you use the console to add the user, you can copy the permissions from an existing user to the new user.

   You can also add a permissions boundary to limit the user's permissions by specifying a policy that defines the maximum permissions that the user can have. Permissions boundaries don't grant any permissions.

For instructions on creating a custom permission policy to use to either grant permissions or set a permissions boundary, see Define custom IAM permissions with customer managed policies.

4. (Optional) Add metadata to the user by attaching tags. For more information about using tags in IAM, see Tags for AWS Identity and Access Management resources.

5. Provide the user with the necessary sign-in information. This includes the password and the console URL for the account sign-in page where the user provides those credentials. For more information, see How IAM users sign in to AWS.

6. (Optional) Configure multi-factor authentication (MFA) for the user. MFA requires the user to provide a one-time-use code each time he or she signs into the AWS Management Console.

7. (Optional) Give IAM users permissions to manage their own security credentials. (By default, IAM users do not have permissions to manage their own credentials.) For more information, see Permit IAM users to change their own passwords.

Note

If you use the console to create the user and you select **User must create a new password at next sign-in (recommended)**, the user has the required permissions.

For information about the permissions that you need in order to create a user, see Permissions required to access IAM resources.

For instructions on creating IAM users for specific use cases, see the following topics:

- Create an IAM user for emergency access
- Create an IAM user for workloads that can't use IAM roles

MFA enabled sign-in

View IAM users

View related pages

Abstracts generated by AI

Location › developerguide

Set up your account

Setting up AWS account, creating administrative user, enabling multi-factor authentication, assigning access permissions, creating permission set, granting unauthenticated access, enabling identity federation.

April 4, 2026

Location › developerguide

[Prerequisites for using Amazon Location Service]

Secure AWS account, create administrative user, assign permissions, grant access to Amazon Location Service, enable unauthenticated access using Amazon Cognito.

April 4, 2026

Batch › userguide

[Create IAM account and administrative user]

Creating AWS account, securing root user, enabling multi-factor authentication, granting administrative access via IAM Identity Center, creating permission set.

April 4, 2026

Discover highly rated pages

Abstracts generated by AI

IAM › UserGuide

[What is IAM?]

IAM controls access, manages permissions, sets up identities, authenticates, authorizes operations on AWS resources, replicates data across data centers.

April 5, 2026

IAM › UserGuide

[Security best practices in IAM]

Apply least-privilege permissions, use IAM roles, MFA, Access Analyzer, guardrails, boundaries.

April 5, 2026

IAM › UserGuide

[IAM Identities]

IAM identities—users, groups, roles—link policies defining authorized AWS actions, resources, conditions.

April 5, 2026

- **Related resources**

- Recommended tasks
- Did this page help you?
-
