

AWS Identity and Access Management



User Guide

Documentation - This Guide

Search

[+ What Is IAM?](#)[□ Getting Set Up](#)[+ Getting Started](#)[+ Tutorials](#)[+ Best Practices and Use Cases](#)[+ IAM Console and Sign-in Page](#)[- Identities](#)[+ Users](#)[+ Groups](#)[- Roles](#)[□ Terms and Concepts](#)[+ Common Scenarios](#)[+ Identity Providers and](#)[AWS Documentation](#) » [AWS Identity and Access Management](#) » [User Guide](#) » [Identities \(Users, Groups, and Roles\)](#) » [IAM Roles](#)

IAM Roles

An IAM *role* is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them). Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.

For these scenarios, you can delegate access to AWS resources using an *IAM role*. This section introduces roles and the different ways you can use them, when and how to choose among approaches, and how to create, manage, switch to (or assume), and delete roles.

Topics

- [Roles Terms and Concepts](#)
- [Common Scenarios for Roles: Users, Applications, and Services](#)

[- Creating IAM Roles](#)

- [Using IAM Roles](#)
- [Managing IAM Roles](#)
- [How IAM Roles Differ from Resource-based Policies](#)