

Choosing an AWS identity service



Choosing an AWS identity service: AWS Decision Guide

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Decision guide **1**

Introduction 1

Understand 2

Identity 3

Authentication 4

Authorization 4

Consider 6

Choose 10

Use 13

Explore 18

Document history **19**

Choosing an AWS identity service

Taking the first step

Time to read	27 minutes
Purpose	Help determine which AWS identity service is the best fit for your organization.
Last updated	January 17, 2025
Covered services	<ul style="list-style-type: none">• Amazon Cognito• AWS Directory Service• AWS Identity and Access Management• IAM Identity Center• AWS Organizations• AWS Resource Access Manager• Amazon Verified Permissions

Introduction

AWS identity services are crucial for establishing secure and manageable access as you begin your AWS journey.

First steps

AWS Identity and Access Management (IAM) is typically the first step, where users create and enforce policies that control access to resources. By establishing IAM best practices—like requiring human users to use federation with an identity provider, using groups, and following the principle of least privilege—organizations can build a secure foundation.

Scaling

As needs grow, other AWS identity services add functionality. For example, AWS IAM Identity Center centralizes access management, helping teams easily manage permissions in complex

environments. AWS Directory Service extends existing on-premises Microsoft Active Directory structures, enabling seamless integration and enhancing security. You can use Amazon Cognito to provide secure, user-friendly access for external users to applications that you build on AWS and need sign-in and sign-up features.

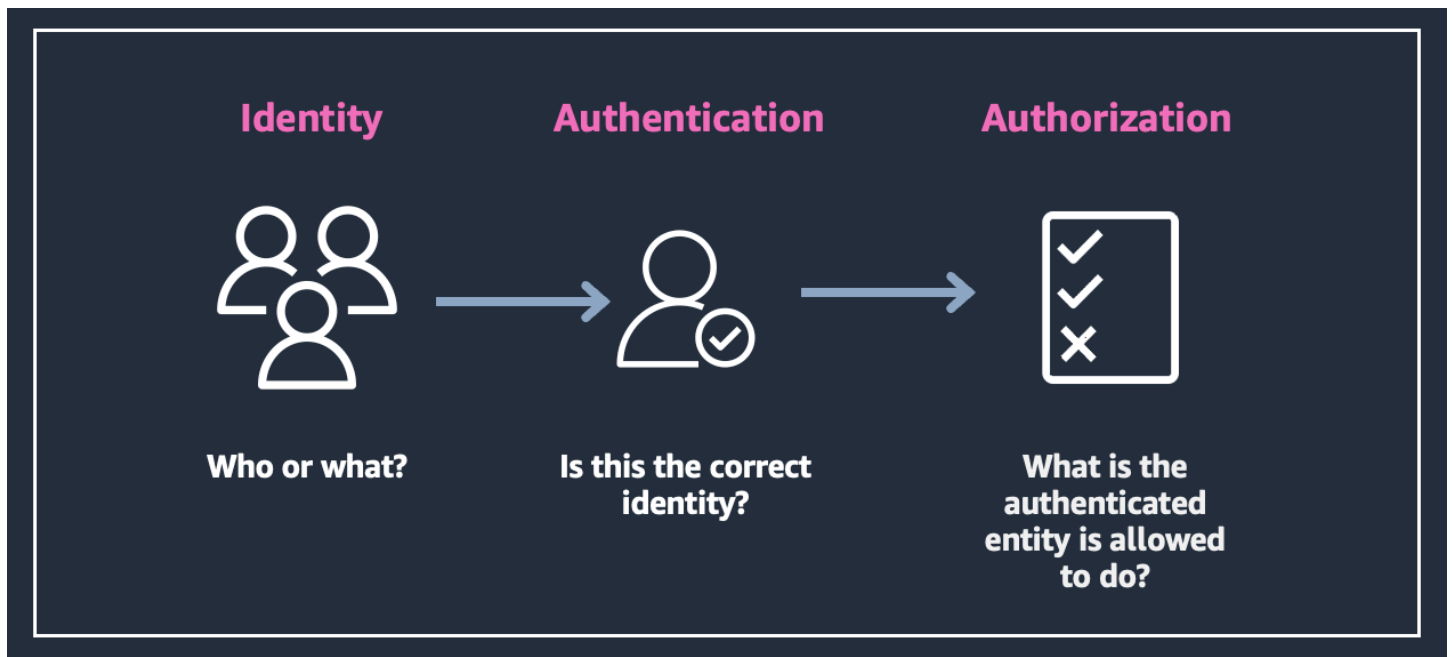
Each identity service plays a role in enhancing security, scalability, and ease of management, making your AWS environments safer and more efficient. Leveraging these services from the beginning supports long-term growth by securing resources, improving operational efficiency, and helping you maintain structured and secure access as you scale.

About this guide

This decision guide helps you get started and choose the right AWS identity service for your use case.

Understand AWS identity services

Let's start by understanding the difference between identity, authentication, and authorization. As shown in the following diagram, **identity** is the unique identification of an entity, **authentication** is the process of verifying the identity, and **authorization** is the process of determining what the authenticated entity is allowed to do.



Another way to think of these concepts is entry to a conference. Your identity is on your credential, which is a government-issued ID. Authentication occurs when the security guard checks your

credential upon entry. Authorization occurs when the guard gives you a wristband that indicates which areas and activities you can attend at this conference.

Note

It's important to follow best practices for identity, authentication, and authorization, such as applying least-privilege permissions, requiring multi-factor authentication, and managing human and machine users differently. The following are helpful resources:

- [Security best practices in IAM](#) in the *AWS Identity and Access Management User Guide*
- [Best practices for a multi-account environment](#) in the *AWS Organizations User Guide*
- [Identity and access management](#) in the *AWS Well-Architected Framework*

The following subsections provide additional detail on AWS services for identity, authentication, and authorization. You can use these services individually, or combined with other services. We'll explore these choices further in the [Choose](#) section.

Identity on AWS

Identity assigns a unique identification to an entity, such as a user, application, or system.

You can manage identity on AWS by using the following services.

IAM Identity Center

[IAM Identity Center](#) is the recommended AWS service for connecting [workforce users](#) to AWS resources, such as AWS-managed applications. It also connects with Microsoft Active Directory through AWS Directory Service.

IAM roles

We recommend using [IAM roles](#) to delegate access to human users, applications, or services that don't normally have access to your AWS resources. IAM roles are IAM identities that have specific permissions and can be assumed by any user, application, or service that needs it.

AWS Directory Service

For AWS customers who use Microsoft Active Directory, [AWS Directory Service](#) provides multiple ways to use Microsoft Active Directory with other AWS services. This allows your

human and machine users to access AWS resources and applications using their existing corporate credentials, simplifying identity management. You can also use AWS Directory Service administer AWS resources using your existing Active Directory credentials.

Authentication on AWS

Authentication is the first step in the access control process, where the system confirms that the entity attempting to access it is who they claim to be. Authentication is a crucial security mechanism that ensures that only authorized entities can interact with your AWS services and resources.

You can manage authentication on AWS by using the following services.

IAM Identity Center

[IAM Identity Center](#) is the recommended AWS service for centrally managing workforce user access to AWS resources. IAM Identity Center users are granted **temporary credentials** (short-term, limited duration) for accessing AWS resources.

IAM roles

[IAM roles](#) are granted **temporary credentials**. Humans, workloads, and AWS services can assume IAM roles.

AWS STS

You can use [AWS Security Token Service](#), a feature of IAM, to create and provide trusted users with **temporary credentials** that can control access to your AWS resources.

Amazon Cognito

[Amazon Cognito](#) provides credentials for web and mobile apps by using user pools and identity pools. Create a [user pool](#) when you want to authenticate and authorize users to your **app or API**, and create an [identity pool](#) when you want to authorize authenticated or anonymous users to access your **AWS resources**.

Authorization on AWS

Authorization is based on the identity that has been authenticated. This identity is used to determine the permissions and access rights. **Permissions** define the specific actions or resources

that an identity is allowed to access or perform. These permissions are typically defined in **policies**, which are used to grant or deny specific actions on AWS resources to users, groups, or roles.

You can manage authorization on AWS by using the following services.

IAM Identity Center

[IAM Identity Center](#) is the recommended AWS service for centrally managing workforce user access to AWS resources. You can use [permission sets](#) to simplify how you assign users and groups in your organization access to AWS accounts. Permission sets are stored in IAM Identity Center and **define the level of access** that users and groups have to an AWS account.

IAM roles

We recommend using [policies](#) to grant permissions to IAM roles. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.

Amazon Cognito

[Amazon Cognito](#) provides credentials for web and mobile apps by using user pools and identity pools. Create a [user pool](#) when you want to authenticate and authorize users to your **app or API**, and create an [identity pool](#) when you want to authorize authenticated or anonymous users to access your **AWS resources**.

Organizations

[AWS Organizations](#) is an account management service that you can use to **consolidate and centrally manage your AWS accounts**. AWS Organizations is recommended, but not required, for use with IAM Identity Center. When you use these services together, you can centrally manage the access of users and groups across all the AWS accounts within your AWS Organization.

AWS RAM

[AWS Resource Access Manager](#) (AWS RAM) helps you securely share your resources **across AWS accounts**. If your account is managed by AWS Organizations, you can also share resources with the other accounts in your organization.

Verified Permissions

[Amazon Verified Permissions](#) is a scalable, fine-grained permissions management and authorization service for your custom applications. Verified Permissions uses the [Cedar](#) policy language to **define fine-grained permissions** for application users.

Consider criteria for choosing an AWS identity service

Choosing the right identity services on AWS depends on your specific requirements and use cases. Here are some criteria to consider when making your decision.

User type

The user type criteria is crucial in selecting an AWS identity service. It aligns services with specific access needs for internal or external users.

1. **External users** (for example, customers or app users): Amazon Cognito is tailored for external users, providing a customizable, secure user directory with options for social sign-ins (such as Google or Facebook) and multi-factor authentication. This service is ideal for web and mobile app developers who need user authentication directly within their applications.
2. **Internal users** (for example, employees and contractors): IAM, IAM Identity Center, and AWS Directory Service are designed to manage internal user access to AWS resources. IAM provides granular permissions control, while IAM Identity Center offers streamlined single sign-on for employees across multiple AWS accounts and third-party applications. AWS Directory Service is suited for organizations that want to integrate on-premises Microsoft Active Directory, providing seamless, secure access for users already managed within Microsoft Active Directory.

By considering user type, organizations can ensure the right balance of security and user experience.

Access requirements

The access requirements criteria helps determine which AWS identity service best meets your organization's specific access needs, whether for AWS resources or applications.

1. **Access to AWS resources:** For managing permissions to AWS resources like Amazon EC2 or [Amazon Simple Storage Service](#) (Amazon S3), IAM is the primary tool, offering fine-grained access control. IAM Identity Center further simplifies access across multiple AWS accounts and provides a centralized way to manage permissions across environments.
2. **Access to applications:** If the goal is to manage sign-in and permissions within applications (such as a mobile or web app for customers), Amazon Cognito is the preferred choice. It offers a secure, user-friendly solution with support for social logins and custom sign-up flows. This helps developers to easily integrate authentication and user management.

3. **Hybrid scenarios:** AWS Directory Service bridges AWS and on-premises Microsoft Active Directory, supporting users who need secure, unified access to both AWS resources and traditional corporate systems.

Selecting your identity services based on access requirements helps you to ensure optimal security and user convenience.

Multi-account management

The multi-account management criteria helps organizations manage permissions, policies, and resource sharing efficiently across multiple AWS accounts, which is essential for scaling and security.

1. **Centralized management and governance:** AWS Organizations is ideal for managing a multi-account environment. You can centrally define policies, apply security controls, and organize accounts into logical structures. It simplifies tasks such as enforcing service control policies (SCPs) and standardizing configurations.
2. **Unified access control:** IAM Identity Center provides single sign-on across multiple accounts, giving users streamlined access based on roles and centralizing identity management.
3. **Resource sharing across accounts:** AWS RAM enables secure sharing of resources like VPCs, subnets, and transit gateways across accounts, reducing duplication and enhancing cost efficiency.

Together, these services can help organizations maintain centralized, secure access and efficient resource management across multiple accounts. This can help streamline operations and improve security posture in complex AWS environments.

Scalability and complexity

The scalability and complexity criteria focuses on selecting AWS identity services that can grow with your organization while effectively managing complexity.

1. **Granular access control:** For precise permissions management, IAM provides highly detailed access controls for users, roles, and resources. It's ideal for fine-tuning access in complex, large-scale environments. However, it might require more in-depth management for large teams or multi-account setups.
2. **Centralized and simplified management:** IAM Identity Center is optimized for multi-account environments, making it scalable for organizations with many users that need unified, role-

based access across various accounts and applications. It reduces complexity by centralizing authentication, especially in hybrid or federated identity structures.

3. **Resource sharing and cost efficiency:** AWS RAM enhances scalability by allowing shared access to resources across accounts. This helps to minimize duplication and support efficient, large-scale architectures.

Selecting identity services based on scalability and complexity can help you maintain manageable and secure identity management as your AWS environment expands.

Integration needs

The integration needs criteria focuses on compatibility with existing identity systems and requirements for unified management across platforms.

1. **On-premises integration:** AWS Directory Service is designed to integrate AWS resources with existing Microsoft Active Directory environments, providing a seamless extension for organizations with established Microsoft Active Directory infrastructure. This service supports common Microsoft Active Directory-based security policies and simplifies access management across on-premises and cloud resources.
2. **Single sign-on for cloud applications:** IAM Identity Center enables SSO access across AWS accounts and third-party applications (such as Microsoft 365 and Salesforce). This can help you to centralize authentication and improve user experience when managing multiple SaaS applications.
3. **Application-level integration:** Amazon Cognito allows integration of secure sign-in and user management features directly within applications. This includes support for social identity providers (such as Google and Facebook) and custom identity providers.

Choosing services based on integration needs ensures smoother operation and unified user access, accommodating both legacy systems and cloud-native environments.

User experience

The user experience criteria emphasizes providing smooth, intuitive access for both administrators and end users.

1. **Single sign-on and simplified access:** IAM Identity Center enhances the user experience so that employees can access multiple AWS accounts and integrated applications through a

single set of credentials. This centralized approach reduces login friction and supports faster access to necessary resources, especially in environments with extensive app usage.

2. **Customizable user authentication:** Amazon Cognito offers a flexible, user-friendly experience tailored for app users. This helps to enable custom branding and support for social logins (such as Google and Facebook) to streamline sign-up and sign-in flows. Amazon Cognito also supports multi-factor authentication, adding an extra layer of security with minimal disruption.
3. **Consistent policy application:** IAM fine-grained permissions allow consistent, role-based access control, so that users only see relevant resources, which improves usability and reduces confusion.

Prioritizing user experience in identity service choice boosts productivity and security.

Security and compliance

The security and compliance criteria helps organizations choose AWS identity services that align with regulatory requirements and enhance security practices.

1. **Granular permissions and access control:** IAM enables detailed permissions management, so that organizations can implement the principle of least privilege. This control is crucial for meeting strict security policies and compliance standards in regulated industries.
2. **Centralized policy enforcement:** AWS Organizations facilitates compliance by applying SCPs across accounts, helping you set consistent security standards and restricted access to sensitive resources. IAM Identity Center complements this by centralizing user access and authentication, supporting compliance with secure sign-on protocols.
3. **Integration with corporate policies:** AWS Directory Service seamlessly extends on-premises Microsoft Active Directory to AWS. This helps you maintain existing security policies and support compliance with regulations that require directory-based authentication.
4. **Enhanced application security:** Amazon Cognito supports multi-factor authentication and customizable policies. You can use Amazon Cognito to secure user access to applications and help developers meet compliance needs for customer data protection.

Selecting identity services based on security and compliance helps to ensure that identity management practices meet industry regulations and organizational standards.

Choose which AWS identity services to use

It's now time to choose which services you want to use for identity, authentication, and authorization. The following sections provide criteria and recommended approaches for common scenarios.

Getting started



When you first get started on AWS, you'll [create an account](#). Doing so will create a [root user](#) in IAM, where you sign in with the email address and password that you used to create the account. The root user has complete access to all AWS services and resources in the account.


Important

We strongly recommend that you don't use the root user for your everyday tasks and that you follow the [root user best practices for your AWS account](#). Only use the root user for [tasks that require root user credentials](#).

Common scenarios

Scenario	What do you want to do?	Recommended service
Creating and managing users for access to AWS	Connect your source of identities or create users, and centrally manage workforce access to multiple AWS accounts and applications	IAM Identity Center
	Enable secure, fine-grained control over access to AWS resources	IAM roles
	Manage multiple workforce users and consolidate billing across your AWS environment	AWS Organizations

Scenario	What do you want to do?	Recommended service
Sharing resources across AWS accounts	Share your resources with other AWS accounts, or within your AWS Organization	AWS Resource Access Manager <div> Note See Shareable AWS resources for a list of which resource types you can share with AWS RAM.</div>
	Control what actions a specified principal can perform on a resource and under what conditions	Resource-based policies <div> Note See Services that work with IAM for a list of which AWS services support resource-based policies.</div>

Scenario	What do you want to do?	Recommended service
Connecting external or federated users	Allow access to your AWS resources using existing corporate credentials such as Microsoft Active Directory	AWS Directory Service for authentication AWS Security Token Service (feature of IAM) for temporary credentials <div>  Note For more information, see Common scenarios for temporary credentials. </div>
	Authenticate and authorize users in your mobile or web app and grant them access to your AWS resources	Amazon Cognito identity pools
Managing fine-grained, centralized access control across your applications	Define fine-grained permissions for authorizing human users to use custom applications	Amazon Verified Permissions
Connecting external or federated machines	Allow machine access to your AWS resources using temporary credentials	AWS Security Token Service (feature of IAM)
Connecting Internet of Things (IoT) devices	Allow IoT device access to your AWS resources	AWS IoT Core
Authenticating using an AWS Software Development Kit (SDK)	See Authentication and access in the <i>AWS SDKs and Tools Reference Guide</i>	

Use AWS identity services

You should now have a clear understanding of each AWS identity service (and the supporting AWS tools and services) and which ones might be the best fit for your organization and use case.

To learn how to use each of the available AWS identity services, we have provided a pathway to explore how each of the services work. The following section provides links to in-depth documentation, hands-on tutorials, and resources to get you started.

Amazon Cognito

- **Guided setup options for Amazon Cognito**

Learn about the most common Amazon Cognito tasks.

[Explore the guide](#)

- **Create a new application in the Amazon Cognito console**

Create a user pool, which allows your users to sign in to your web or mobile app.

[Get started with the tutorial](#)

- **Create an identity pool**

Create an identity pool, which allows your users to obtain temporary AWS credentials to access AWS services.

[Get started with the tutorial](#)

- **Amazon Cognito workshop**

Practice using Amazon Cognito to build an authentication solution for a hypothetical pet store.

[Get started with the tutorial](#)

AWS Directory Service

- **Getting started with AWS Directory Service**

Learn how to create a fully managed Microsoft Active Directory in the AWS Cloud.

[Explore the guide](#)

- **AWS Managed Microsoft AD best practices**

Read suggestions and guidelines to avoid problems and get the most out of AWS Managed Microsoft AD.

[Explore the guide](#)

- **AWS Directory Service Pricing**

Understand the costs associated with AWS Directory Service offerings. Includes a pricing calculator to determine your AWS Directory Service and architecture cost in a single estimate.

[Explore the guide](#)

- **AWS Directory Service FAQ**

Deep dive into the AWS Directory Service through exploring the FAQ.

[Explore the guide](#)

IAM

- **Getting started with IAM**

Create IAM roles, users, and policies using the AWS Management Console.

[Get started with the tutorial](#)

- **Delegate access across AWS accounts using roles**

Use a role to delegate access to resources in different AWS accounts that you own.

[Get started with the tutorial](#)

- **Create a customer managed policy**

Use the AWS Management Console to create a customer managed policy and then attach that policy to an IAM user in your AWS account.

[Get started with the tutorial](#)

- **Define permissions to access AWS resources based on tags**

Create and test a policy that allows IAM roles with principal tags to access resources with matching tags.

[Get started with the tutorial](#)

- **Cross account resource access in IAM**

Understand how to share resources by using resource-based policies.

[Explore the guide](#)

- **Security best practices in IAM**

Help secure your AWS resources by using IAM best practices.

[Explore the guide](#)

IAM Identity Center

- **Enabling AWS IAM Identity Center**

Enable IAM Identity Center and begin using it with your AWS Organizations.

[Explore the guide](#)

- **Configure user access with the default IAM Identity Center directory**

Use the default directory as your identity source and set up and test user access.

[Get started with the tutorial](#)

- **Using Active Directory as an identity source**

Complete the basic setup for using Microsoft Active Directory as an IAM Identity Center identity source.

[Get started with the tutorial](#)

- **Configure SAML and SCIM with Okta and IAM Identity Center**

Set up a SAML connection with Okta and IAM Identity Center.

[Get started with the tutorial](#)

Organizations

- **Creating and configuring an organization**

Create your organization and configure it with two AWS member accounts.

[Get started with the tutorial](#)

- **AWS services that you can use with AWS Organizations**

Understand which AWS services you can use with AWS Organizations, and the benefit of using each service on an organization-wide level.

[Explore the guide](#)

- **Organizing your AWS environment using multiple accounts**

Implement best practices and current recommendations for organizing your overall AWS environment.

[Read the whitepaper](#)

AWS RAM

- **Getting started with AWS RAM**

Learn about AWS RAM terms and concepts.

[Explore the guide](#)

- **Working with shared AWS resources**

Share AWS resources that you own, and access AWS resources that are shared with you.

[Explore the guide](#)

- **Managing permissions in AWS RAM**

Learn about the two types of managed permissions: AWS managed permissions and customer managed permissions.

[Explore the guide](#)

- **Configure detailed access to your resources that are shared using AWS RAM**

Use customer managed permissions to customize your resource access and achieve the best practice of least privilege.

[Read the blog](#)

Verified Permissions

- **Create your first Verified Permissions policy store**

Create a sample policy store by using the Verified Permissions console.

[Explore the guide](#)

- **Best practices for designing an authorization model**

Ask yourself questions to define your principals, resources, actions, and how they interrelate to each other.

[Explore the guide](#)

- **Use Amazon Verified Permissions for fine-grained authorization at scale**

Learn how you can provide a faster and richer user experience while still authorizing all requests in the application. You will learn two techniques—*bulk authorization* and *response caching*—to improve the efficiency of your applications.

[Read the blog](#)

- **Amazon Verified Permissions pricing**

Learn about Amazon Verified Permissions pricing, including several pricing examples.

[Explore the guide](#)

- **Amazon Verified Permissions FAQ**

Deep dive into Amazon Verified Permissions by exploring the FAQ.

[Explore the guide](#)

Explore applications of AWS identity services

This section suggests editable architecture diagrams, ready-to-use code, and documentation to help you apply AWS identity services.

Editable architecture diagrams

Reference architecture diagrams

Explore reference architecture diagrams to help you develop your identity strategy.

[Explore security, identity, and governance reference architectures](#)

Ready-to-use code

AWS Solutions

Explore pre-configured, deployable solutions and their implementation guides, built by AWS.

[Explore all AWS security, identity, and governance solutions](#)

Documentation

Security, identity, and governance whitepapers

Explore whitepapers for further insights and best practices on choosing, implementing, and using the identity services that best fit your organization.

[Explore security, identity, and governance whitepapers](#)

AWS Security Blog

Explore blog posts that address specific security use cases.

[Explore the AWS Security blog](#)

Document history

The following table describes the important changes to this decision guide. For notifications about updates to this guide, you can subscribe to an RSS feed.

Change	Description	Date
Initial publication	Guide first published.	January 17, 2025