

Q Search in this guide

Documentation > AWS IAM Identity Center > User Guide

Contact Us

English ▼

Create an AWS Account

Feedback 📮

Preferences 🔞

AWS IAM Identity

Center
User Guide

What is IAM Identity Center?

- ► Enabling IAM Identity Center
- Common tasks
- ▶ Identity source tutorials
- ► IAM Identity Center instances

 Authentication in IAM Identity

 Center
- Connect workforce users
- Application access
- ▶ AWS account access
- Resiliency design and Regional behavior
- Security
- ▶ Tagging resources

Integrating AWS CLI with IAM Identity Center

Region availability

Considerations for Private Access

Quotas

Troubleshooting

Document history

AWS Glossary

What is IAM Identity Center?

PDF RSS

AWS IAM Identity Center is the AWS solution for connecting your workforce users to AWS managed applications such as Amazon Q Developer and Amazon QuickSight, and other AWS resources. You can connect your existing identity provider and synchronize users and groups from your directory, or create and manage your users directly in IAM Identity Center. You can then use IAM Identity Center for either or both of the following:

- User access to applications
- User access to AWS accounts

Already using IAM for access to AWS accounts?

You don't need to make any changes to your current AWS account workflows to use IAM Identity Center for access to AWS managed applications. If you're using federation with IAM or IAM users for AWS account access, your users can continue to access AWS accounts in the same way they always have, and you can continue to use your existing workflows to manage that access.

Why use IAM Identity Center?

IAM Identity Center streamlines and simplifies workforce user access to applications or AWS accounts, or both, through the following key capabilities.

On this page

Why use IAM Identity Center?

IAM Identity Center rename

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies cannot be deactivated, but you can click "Customize cookies" to decline performance cookies.

If you agree, AWS and approved third parties will also use cookies to provide useful site features, remember your preferences, and display relevant content, including relevant advertising. To continue without accepting these cookies, click "Continue without accepting." To make more detailed choices or learn more, click "Customize cookies."

Accept all cookies

Continue without accepting

Customize cookies

Documentation > AWS IAM Identity Center > User Guide

•

Contact Us

Create an AWS Account

Feedback 📮 P

Preferences 🔞

managed applications such as
Amazon Redshift and authorize
access to AWS resources based on the
user's identity. You can more easily
audit user activity because CloudTrail
events are logged based on the user
and the actions the user initiated. This
makes it easier to understand who
accessed what. For information about
supported use cases, including endto-end configuration guidance, see
Trusted identity propagation use

One place to assign permissions to multiple AWS accounts

cases.

With multi-account permissions, IAM Identity Center provides a single place for you to assign permissions to groups of users in multiple AWS accounts. You can create permissions based on common job functions or define custom permissions that meet your security needs. You can then assign those permissions to workforce users to control their access to specific AWS accounts.





This optional feature is available only for organization instances of IAM Identity Center.



One point of federation to simplify user access to AWS

By providing one point of federation, IAM Identity Center reduces the administrative effort required to use multiple AWS managed applications and AWS accounts. With IAM Identity Center, you only federate once, and you have only one certificate to manage when using a SAML 2.0 identity provider. IAM Identity Center provides AWS managed applications with a common view of users and groups for trusted identity propagation use cases, or when users

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies cannot be deactivated, but you can click "Customize cookies" to decline performance cookies.

If you agree, AWS and approved third parties will also use cookies to provide useful site features, remember your preferences, and display relevant content, including relevant advertising. To continue without accepting these cookies, click "Continue without accepting." To make more detailed choices or learn more, click "Customize cookies."

Contact Us

Create an AWS Account

Feedback 🗔

Preferences 🔞

Documentation > AWS IAM Identity Center > User Guide

organization instance is the best practice. It's the only instance that enables you to manage access to AWS accounts and it's recommended for all production use of applications. An organization instance is deployed in the AWS Organizations management account and gives you a single point from which to manage user access across AWS.

Account instances are bound to the AWS account in which they are enabled. Use account instances of IAM Identity Center only to support isolated deployments of select AWS managed applications. For more information, see Organization and account instances of IAM Identity Center.

User-friendly web portal access for your users

The AWS access portal is a userfriendly web portal that provides your users with seamless access to all their assigned applications, AWS accounts, or both.

IAM Identity Center rename

On July 26, 2022, AWS Single Sign-On was renamed to AWS IAM Identity Center.

Legacy namespaces remain the same

The sso and identitystore API namespaces along with the following related namespaces **remain unchanged** for backward compatibility purposes.

- CLI commands
 - aws configure sso

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies cannot be deactivated, but you can click "Customize cookies" to decline performance cookies.

If you agree, AWS and approved third parties will also use cookies to provide useful site features, remember your preferences, and display relevant content, including relevant advertising. To continue without accepting these cookies, click "Continue without accepting." To make more detailed choices or learn more, click "Customize cookies."

 Documentation URLs containing singlesignon

Did this Next page help topic: Enabling you? IAM Identity Center **⚠** Yes **♥** No Need help? Try AWS **Provide** re:Post 🛂 feedback Connect with an **AWS IQ** expert 🖸

> Privacy | Site terms | Cookie preferences | © 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies cannot be deactivated, but you can click "Customize cookies" to decline performance cookies.

If you agree, AWS and approved third parties will also use cookies to provide useful site features, remember your preferences, and display relevant content, including relevant advertising. To continue without accepting these cookies, click "Continue without accepting." To make more detailed choices or learn more, click "Customize cookies."