Federation

Archived: 2026-04-06 01:11:29 UTC

AWS IAM Identity Center makes it easy to centrally manage federated access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place. You can use AWS IAM Identity Center for identities in the AWS IAM Identity Center's user directory, your existing corporate directory, or external IdP.

AWS IAM Identity Center works with an IdP of your choice, such as Okta Universal Directory or Azure Active Directory (AD) via the Security Assertion Markup Language 2.0 (SAML 2.0) protocol. AWS IAM Identity Center seamlessly leverages IAM permissions and policies for federated users and roles to help you manage federated access centrally across all AWS accounts in your AWS organization. With AWS IAM Identity Center, you can assign permissions based on the group membership in your IdP's directory, and then control the access for your users by simply modifying users and groups in the IdP. AWS IAM Identity Center also supports the System for Cross-domain Identity Management (SCIM) standard for enabling automatic provisioning of users and groups from Azure AD or Okta Universal Directory to AWS. AWS IAM Identity Center makes it easy for you to implement attribute-based access control (ABAC) by defining fine-grained permissions based on user attributes defined in your SAML 2.0 IdP. AWS IAM Identity Center allows you to select your ABAC attributes from the user information synchronized from the IdP via SCIM or pass multiple attributes, such as cost center, title, or locale, as a part of a SAML 2.0 assertion. You can define permissions once for your entire AWS organization, and then grant, revoke, or modify AWS access by simply changing the attributes in your IdP. With AWS IAM Identity Center, you can also assign permissions based on the group membership in your IdP's directory, and then control the access for your users by simply modifying users and groups in the IdP.

AWS IAM Identity Center can serve as an IdP to authenticate users to AWS IAM Identity Center integrated applications and SAML 2.0 compatible cloud-based applications, such as Salesforce, Box, and Microsoft 365, with a directory of your choice. You can also use AWS IAM Identity Center to authenticate users to the AWS Management Console, AWS Console Mobile Application, and AWS Command Line Interface (CLI). For your identity source, you can choose Microsoft Active Directory or AWS IAM Identity Center's user directory.

To learn more, see the AWS IAM Identity Center User Guide, visit AWS IAM Identity Center Getting Started, and explore the following additional resources:

- Blog post: AWS IAM Identity Center between Okta Universal Directory and AWS
- Blog post: The Next Evolution in AWS IAM Identity Center

Source: https://aws.amazon.com/identity/federation/