5 ways to modernize workforce identity with AWS

Discover secure, scalable, and fine-grained identity and access management controls that improve your security posture and agility

State of the market: Identity in the modern world

Migrating and modernizing applications by moving to the cloud enables lower costs, improves efficiency, and allows organizations to get the most value from their existing investments. To complement this move, organizations need a better way to manage identities, resources, and permissions securely and at scale.

Modern security—in which actual network boundaries extend beyond traditional office spaces—seeks to achieve complementary identity and network controls, with each component augmenting the other. Identity-centric controls in the cloud offer strong, flexible, fine-grained access controls, while network-centric controls provide well-understood perimeters within which identity-centric controls can operate.

Identity and access management has emerged as a key enabler of growth and innovation and data and asset protection; the primary instrument for enforcing best practices in authentication, authorization, and governance; and the foundation for a strong security posture in today's cloud-first world.

For an identity solution to be truly viable, it cannot simply act as a gatekeeper. Modern identity and access management must enable network-centric and identity-centric controls to work in tandem. The two components must augment each other to safeguard workforce users, data, and resources; aid with compliance; and improve performance—all while enhancing productivity and output.

By working backward from specific use cases, organizations can determine the optimal identity and access management approach—balancing areas such as IT investment and end-user impact—to modernize their workforce identity strategy and help achieve their larger security goals.

> ***"Using AWS…we were able to accelerate projects onboarded to cloud by 5X, reduce number of permission tickets by 10X, and experienced 3X fewer stability issues. This is all made possible using simple APIs from AWS Organizations."***
>
> – Gaurav Jain, Former SVP, Sr. Director, Cloud Platform, Factset

Modernizing workforce identity with AWS

Your organization's workforce has varying requirements when it comes to accessing applications, resources, and data:

- Admins need centralized identity provisioning with the flexibility to connect identity providers, provision access controls scoped to least privilege, and integrate visibility and governance into the actions taken across their environments to meet stringent security and compliance requirements
- Architects and developers need frictionless access to AWS resources and services so they can focus on modernizing applications in the cloud
- End users need seamless access to internal applications, collaboration tools, and resources
- Suppliers and partners need access points to collaborate with your teams

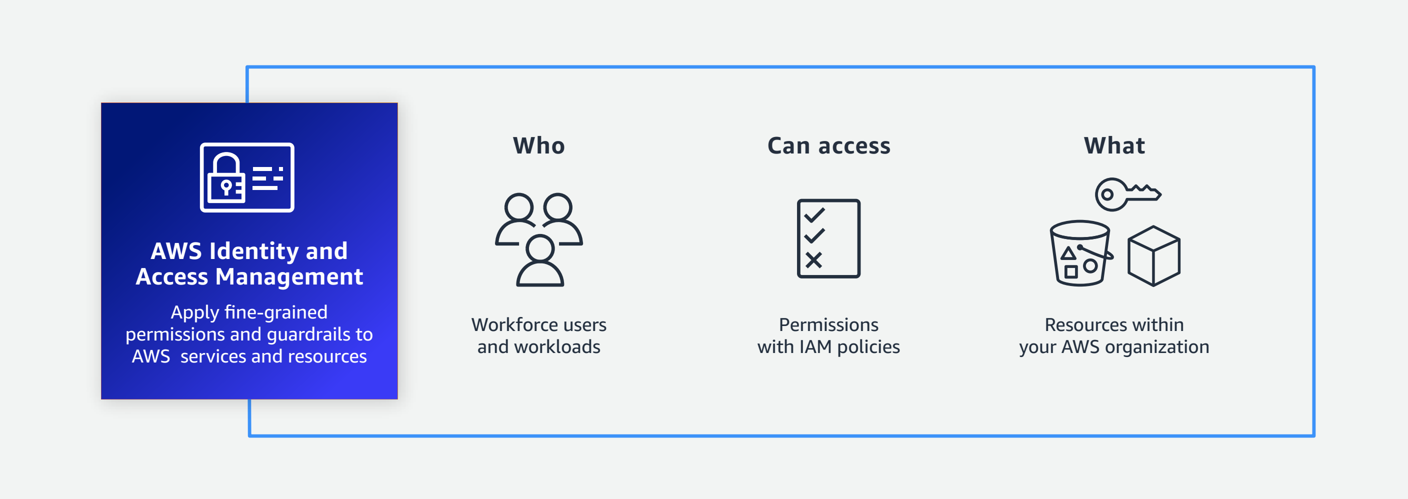
AWS Identity Services enable the freedom to create, connect, and manage identities, resources, and permissions securely, at scale, and in ways designed for the digital-first era. With AWS, you'll get comprehensive workforce identity security throughout your adoption journey while using tools to scale your identity program as you build and innovate.

You can use AWS Identity Services to authenticate, authorize, and centrally govern your environment with the granularity to grant the right access to the right people at the right time. And AWS Identity Services help accelerate cloud adoption, as they allow you to centralize workforce user access from on-premises and the cloud, providing users secure cross-account access—so they can innovate more with AWS applications and services.

At AWS, we recognize that each organization may have unique requirements influencing the design of a foundational architecture. So, we give you options at every level of your workforce identity journey while providing guidance to help you make smart identity and access management decisions with greater ease.

In this eBook, we'll examine five key workforce identity capabilities in AWS—demonstrating how they can help you modernize identity for better security, greater visibility and control, and a more productive workforce.

Figure 1



AWS Identity and Access Management
Apply fine-grained permissions and guardrails to AWS services and resources
Who
Workforce users and workloads
Can access
Permissions with IAM policies
What
Resources within your AWS organization

> *“GE uses AWS Identity Services to support their global enterprise and allow their businesses to operate securely in the cloud. AWS Organizations and Service Control Policies (SCP) provide top-down governance and allows for the delegation of identity based and resource-based policy administration to each business unit. This model allows the businesses to move independently and operate at scale to solve today’s industrial challenges.”*
>
> – Matthew Green, Former VP, Cloud Architecture, GE

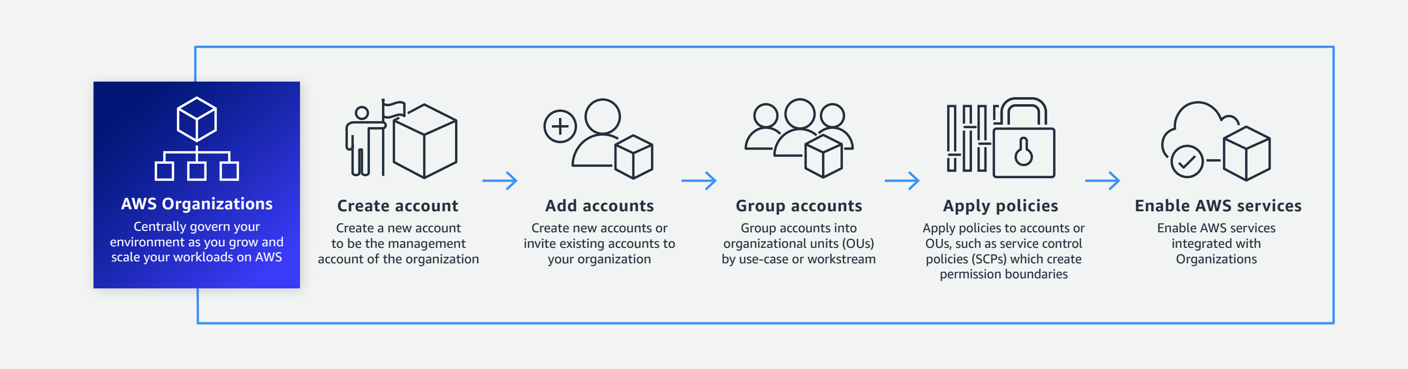
1. Centrally govern your environment to improve compliance

AWS simplifies access and management control. This allows you to establish guardrails and create areas where your teams can build, experiment, and innovate freely within safe boundaries—and without fear of compromising security or regulatory compliance.

For example, you can use guardrails to improve security and consistently enforce which users can use a service or create a certain type of resource or where they can store data. These guardrails form the boundaries within which you can build more fine-grained access controls.

With AWS, you can use **AWS Organizations** to centrally manage AWS accounts and access controls. The resulting organization-wide permissions are the logical intersection of what is allowed by AWS Organizations at the account level and the permissions that are explicitly granted by IAM at the user or role level within that account. With AWS, you also can improve security and maintain compliance by consistently enforcing who can create and access what types of resources and where.

Figure 2



AWS Organizations
Centrally govern your environment as you grow and scale your workloads on AWS
Create account
Create a new account to be the management account of the organization
Add accounts
Create new accounts or invite existing accounts to your organization
Group accounts
Group accounts into organizational units (OUs) by use-case or workstream
Apply policies
Apply policies to accounts or OUs, such as service control policies (SCPs) which create permission boundaries
Enable AWS services
Enable AWS services integrated with Organizations

To quickly start running secure, scalable workloads, use AWS Control Tower to set up and govern a multi-account AWS environment based on best practices by:

Using a landing zone and AWS Organizations for account management and governance with aligned security best practices

Specifying the maximum permissions for member accounts with organization-wide guardrails using service control policies (SCPs)

Restricting which AWS services, resources, and individual API actions the users and roles in each member account can access

Defining conditions for when to restrict access—with restrictions that override member account admins

Providing an integrated dashboard so you can see a top-level summary of policies applied to your multi-account AWS environment

Blocking access to services, resources, or API actions for member accounts—with blocks that remain in effect even when member account admins explicitly grant such permissions

> *"AWS...allowed us to centralize authentication to our Identity provider (IdP), which has been a massive improvement on a daily basis for our employees... Our infrastructure security team was also able to centralize access management, resulting in an increase in platform security and a decrease in operational costs."*
>
> – Rocco Zanni, CTO, Spreaker

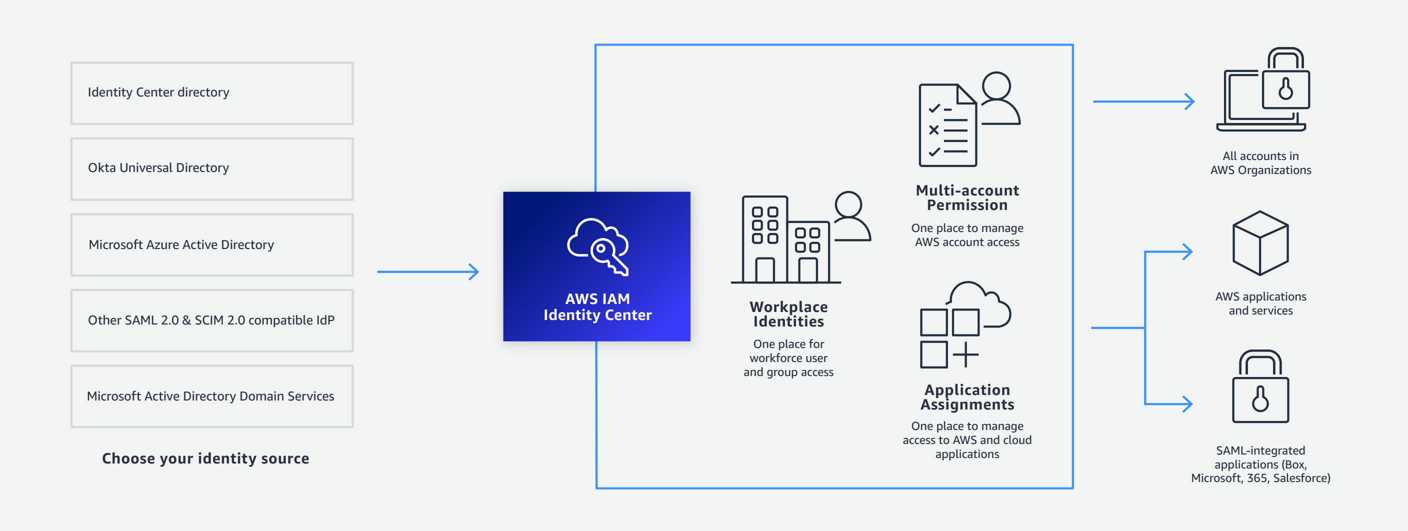
2. Simplify access management with AWS

AWS provides your administrators with the freedom to centrally create and/or connect identities in AWS to help you grow and scale with confidence. You can manage the access of your workforce identities across multiple AWS accounts and applications, all from a singular, unified console: **AWS IAM Identity Center** (the successor to AWS Single Sign-On, or AWS SSO).

AWS IAM Identity Center allows you to:

- Choose your preferred identity source for use across AWS
- Use multi-account permissions to give workforce users access to multiple AWS accounts
- Use the power of application assignments to give your workforce users single sign-on access to AWS and cloud applications

Figure 3


Identity Center directory
Okta Universal Directory
Microsoft Azure Active Directory
Other SAML 2.0 & SCIM 2.0 compatible IdP
Microsoft Active Directory Domain Services
Choose your identity source
AWS IAM Identity Center
Workplace Identities
One place for workforce user and group access
Multi-account Permission
One place to manage AWS account access
Application Assignments
One place to manage access to AWS and cloud applications
All accounts in AWS Organizations
AWS applications and services
SAML-integrated applications (Box, Microsoft, 365, Salesforce)

AWS enables you to quickly grant the right access to the right people at the right time by selecting permissions from a library of **AWS managed policies**, which you can use as starting points to create your own custom-managed policies. You can also leverage existing APIs to automate such actions based on their organizational policies, apart from ability to take manual actions.

AWS provides access to a cloud platform supporting and providing flexible solutions to today's access control challenges through **Attribute-based Access Control** (ABAC). This powerful enterprise-ready model has been proven to define and manage fine-grained, highly customizable user permissions.

Finally, AWS helps you continuously improve your security posture by analyzing access patterns and identifying unused permissions across all AWS accounts—so you can remove unnecessary access quickly and confidently. Wherever you are in your cloud adoption journey, AWS offers the right mix of workforce identity tools inside and outside AWS to help you meet your security and business goals.

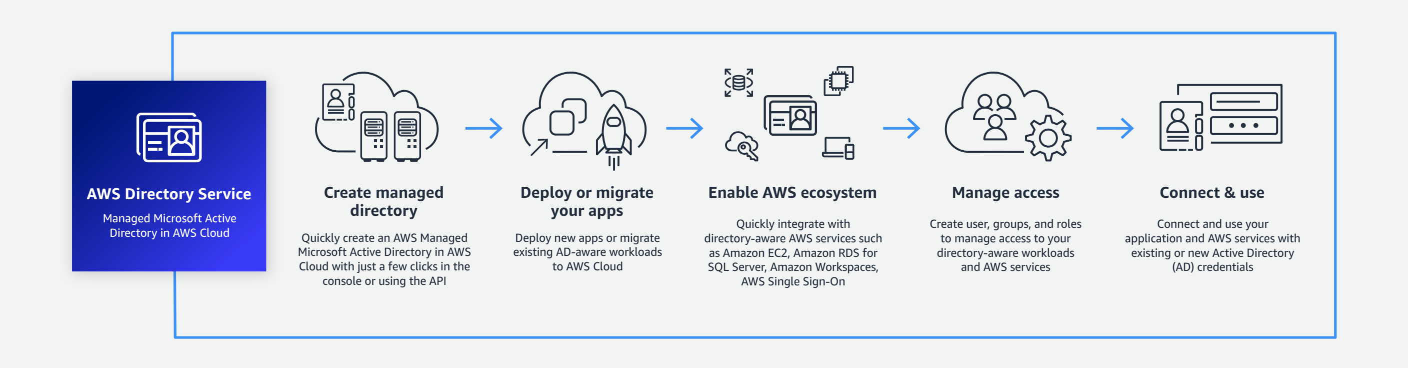
> *"AWS Managed AD allows us to leverage a trust relationship with our on-premises directory, allowing our AWS resources to utilize either directory for authentication. AWS…enables us to easily onboard new accounts and users, saving us days if not weeks of effort."*
>
> – John Wagenleitner, Technical Architect/Developer, CSU, Fresno

3. Enable app modernization with existing assets

By setting AWS Directory Service for Microsoft Active Directory as the identity source for **AWS IAM Identity Center**, you can grant AD users and groups access to AWS accounts and applications by simply adding them to the appropriate Active Directory groups.

For example, say you decide to grant a DevOps group access to your production AWS accounts. Users added to the DevOps group are then granted single sign-on access to these AWS accounts automatically. This automation makes it easy to onboard new users and gives existing users access to modernize new accounts and applications quickly.

Figure 4



AWS Directory Service

Managed Microsoft Active Directory in AWS Cloud

Create managed directory

Quickly create an AWS Managed Microsoft Active Directory in AWS Cloud with just a few clicks in the console or using the API

Deploy or migrate your apps

Deploy new apps or migrate existing AD-aware workloads to AWS Cloud

Enable AWS ecosystem

Quickly integrate with directory-aware AWS services such as Amazon EC2, Amazon RDS for SQL Server, Amazon Workspaces, AWS Single Sign-On

Manage access

Create user, groups, and roles to manage access to your directory-aware workloads and AWS services

Connect & use

Connect and use your application and AWS services with existing or new Active Directory (AD) credentials

AWS IAM Identity Center also makes it simple for you to manage single sign-on for your workforce across all AWS accounts and integrated applications and custom SAML 2.0-based applications—without custom scripts. You can use application assignments in AWS IAM Identity Center to quickly assign which workforce users should have one-click access to only the applications that you've authorized and get users on their path to application modernization.

> ***“Using AWS Organizations, GoDaddy is able to implement consistent security guardrails across accounts, while giving our application teams the flexibility to build at their own accelerated pace.”***
>
> – Ketan Patel, Senior Director, Software Development, GoDaddy

4. Implement the principle of least privilege

Protect your data and resources by building organization-wide permissions guardrails and fine-grained access controls across your groups, roles, and resources in AWS. You can use a mix of policy types and inspect, test, validate, and refine these policies across your identities and resources as you work toward least privilege.

With AWS, you can quickly inspect and refine policies across your identities and resources using **AWS IAM Access Analyzer**. Set fine-grained permissions, verify intended permissions, and refine permissions by removing unused access. These strong-layered defenses help streamline permissions management throughout every step of your least privilege journey.

AWS makes it easy to identify over-privileged roles and resources in your AWS accounts, validate the IAM policies associated with those resources, and generate new policies based on access activity.

Accelerate your journey to least privilege

Learn how to apply least privilege permissions on AWS, use AWS IAM Access Analyzer to set, verify, and refine fine-grained permissions, and more.

Watch the AWS re:Invent 2021 session

5. Improve your security posture with strong identity practices

Strong identity-centric controls, like authentication and authorization, form the basis of the security model between AWS services. With AWS, you have the option to add a variety of **multi-factor authentication (MFA) mechanisms** for when your workforce users access AWS applications and services. AWS supports virtual MFA devices, U2F, and hardware MFA devices.

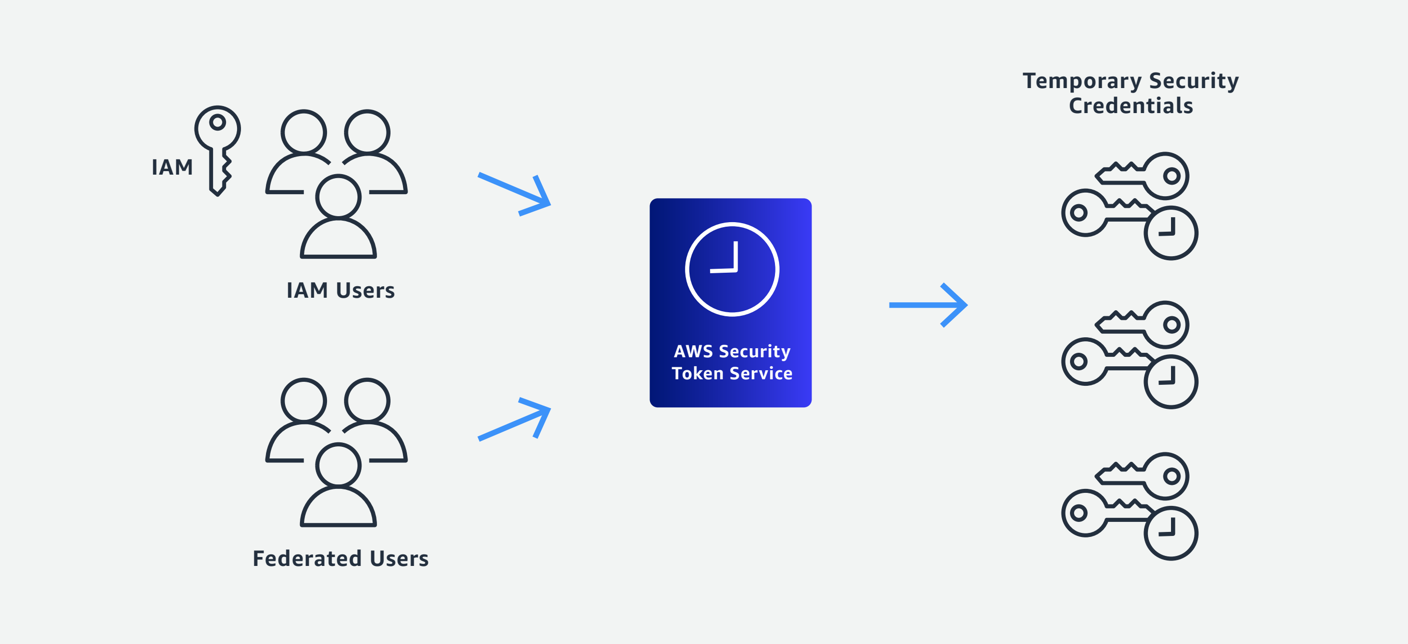
You also get access control granularity to meet stringent requirements—from organization-wide permissions guardrails to fine-grained access control. With AWS, you can inspect, test, validate, and refine access policies across your identities and resources. Cloud admins, resource managers, and organizational owners have broad controls to meet security and compliance requirements.

And with **IAM roles**, you can provide trusted users with temporary security credentials that can control access to your AWS resources. These work almost identically to the long-term access key credentials held by your IAM users but with just a few differences. Temporary security credentials on AWS:

- Can be configured to last anywhere from a few minutes to several hours
- Will not be recognized by AWS nor allowed any kind of API requests made from them after they expire
- Are dynamically generated and provided to the user when requested rather than being stored with the user

Additionally, users can request new credentials after (or even before) their temporary credentials expire—so long as they have permission to do so.

Figure 5



Get started modernizing your workforce identity with AWS

In today's increasingly distributed, remote, cloud-first world, identity has emerged as a critical enabler of business success and a competitive differentiator that provides a powerful edge. Organizations that embrace modern approaches to identity and access management will move with greater speed and agility.

Workforce Identity in AWS enables modern identity and access management that saves time, improves productivity, and empowers your organization to innovate more securely in your AWS environment.

With AWS, you can help ensure regulatory compliance with greater ease through central governance. Gain centralized identity management and fine-grained access control for improved data protection, privacy, and productivity. Leverage your existing identity source to quickly modernize your applications. Build a journey toward the principle of least privilege with streamlined, fine-grained permissions management. And use strong identity practices to grant access with greater ease and security, save time, and eliminate extra work.

Your journey to modern workforce identity in AWS starts today.

Dive into identity practices within the AWS Well-Architected Framework ›