

AWS Identity and Access Management

Securely manage identities and access to AWS services and resources

Why use IAM?

Use AWS Identity and Access Management (IAM) to manage and scale workload and workforce access securely supporting your agility and innovation in AWS.



Benefits of IAM

Set permission guardrails and fine-grained access

Set and manage guardrails with broad permissions, and move toward least privilege by using fine-grained access controls for your workloads.

Manage workload and workforce identities across your AWS accounts

Manage identities across single AWS accounts or centrally connect identities to multiple AWS accounts.

Use temporary security credentials and permission sets to access your AWS resources

Grant temporary security credentials for workloads that access your AWS resources using IAM and grant your workforce access with AWS IAM Identity Center.

Analyze access and validate IAM policies as you move toward least privilege

Generate least-privilege policies, verify external and unused access to resources, and continually analyze to rightsize permissions.

Use cases

Apply fine-grained permissions and scale with attribute-based access control

Create granular permissions based on user attributes—such as department, job role, and team name—by using attribute-based access control.

[Learn about attribute-based access control](#)

Manage per-account access or scale access across AWS accounts and applications

Manage per-account identities with IAM or use IAM Identity Center to provide multi-account access and application assignments across AWS.

[Learn about centralizing identity and access management](#)

Establish organization-wide and preventative guardrails on AWS

Use [service control policies](#) to establish permissions guardrails for IAM users and roles, and implement a data perimeter around your accounts in AWS Organizations.

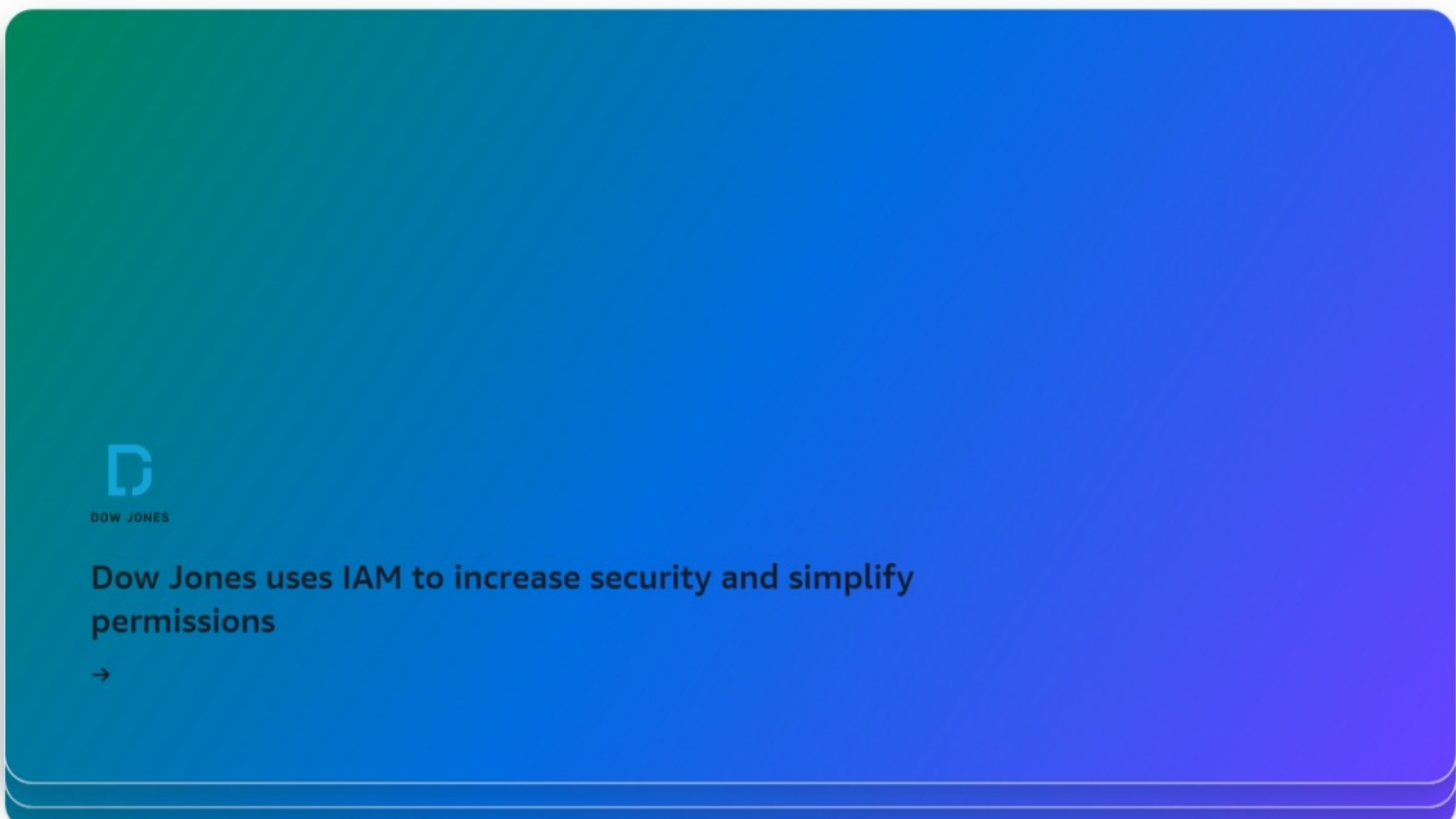
[Learn about data perimeter guardrails](#)

Set, verify, and right-size permissions toward least privilege

Streamline permissions management and use cross-account findings as you set, verify, and refine policies on the journey toward least privilege.

[Learn about the least-privilege journey](#)

Customers



Next steps

Did you find what you were looking for today?

Let us know so we can improve the quality of the content on our pages

Learn

What Is AWS?
What Is Cloud Computing?
What Is Agentic AI?
Cloud Computing Concepts Hub
AWS Cloud Security
What's New
Blogs
Press Releases

Resources

Getting Started
Training
AWS Trust Center
AWS Solutions Library
Architecture Center
Product and Technical FAQs
Analyst Reports
AWS Partners

Developers

Builder Center
SDKs & Tools
.NET on AWS
Python on AWS
Java on AWS
PHP on AWS
JavaScript on AWS

Help

Contact Us
File a Support Ticket
AWS rePost
Knowledge Center
AWS Support Overview
Get Expert Help
AWS Accessibility
Legal

Back to top