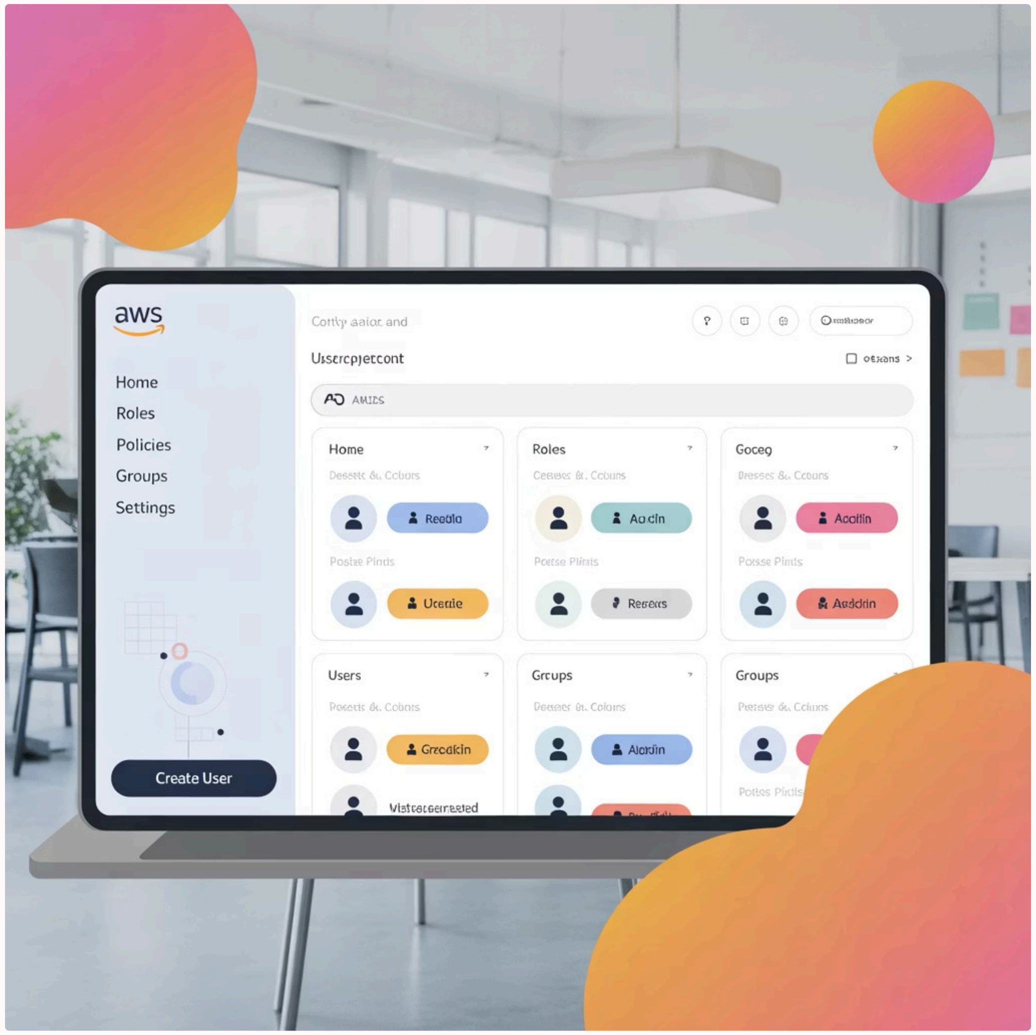
AWS Access Management: Capabilities Overview

Welcome to our comprehensive guide to AWS access management capabilities. We'll explore how AWS helps organizations secure their cloud resources through sophisticated access controls while maintaining regulatory compliance in today's complex security landscape.

Introduction to AWS IAM

AWS Identity and Access Management (IAM) is the cornerstone of security in AWS cloud environments. This centralized service enables precise control over who can access which AWS resources and under what conditions.

IAM follows a default deny principle: all access requests are automatically denied unless explicitly permitted through policies. This security-first approach ensures resources remain protected by default.



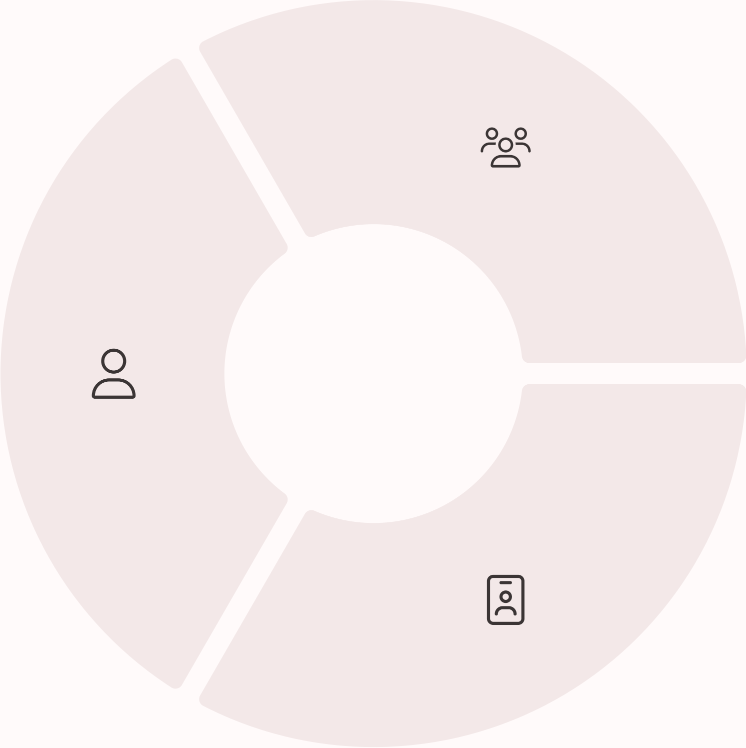
Global Service

IAM operates across all AWS regions, providing consistent security controls worldwide

Free to Use

There are no additional charges for using IAM to manage access to your AWS resources

Managing Users, Groups, and Roles



IAM Users

Entities that represent people or applications needing AWS access

- Unique credentials for authentication
- Long-term access keys for programmatic access
- Individual permission sets based on job function

IAM Groups

Collections of IAM users for simplified permission management

- Assign permissions to entire teams at once
- Simplifies administration of large user bases
- Users can belong to multiple groups simultaneously

IAM Roles

Temporary permission sets assumed by users or services

- No permanent credentials attached
- Enables cross-service and cross-account access
- Perfect for temporary elevated privileges

Granular Permissions and Policy Management

Policies are written in JSON format, defining permissions that specify what actions are allowed or denied on which resources and under what conditions.

Identity-Based Policies

Attached directly to users, groups, or roles to control what actions they can perform on which resources

Resource-Based Policies

Attached directly to resources like S3 buckets or SQS queues to control who can access that specific resource

Permission Boundaries

Set the maximum permissions an identity can have, regardless of policies attached to them

Service Control Policies

Used with AWS Organizations to define permission guardrails across multiple accounts

Authentication and Multifactor Security

Standard Authentication

Basic username and password credentials for AWS Management Console access

- Customizable password policies (length, complexity, rotation)
- Access keys for programmatic access via API, CLI, or SDK

Multi-Factor Authentication

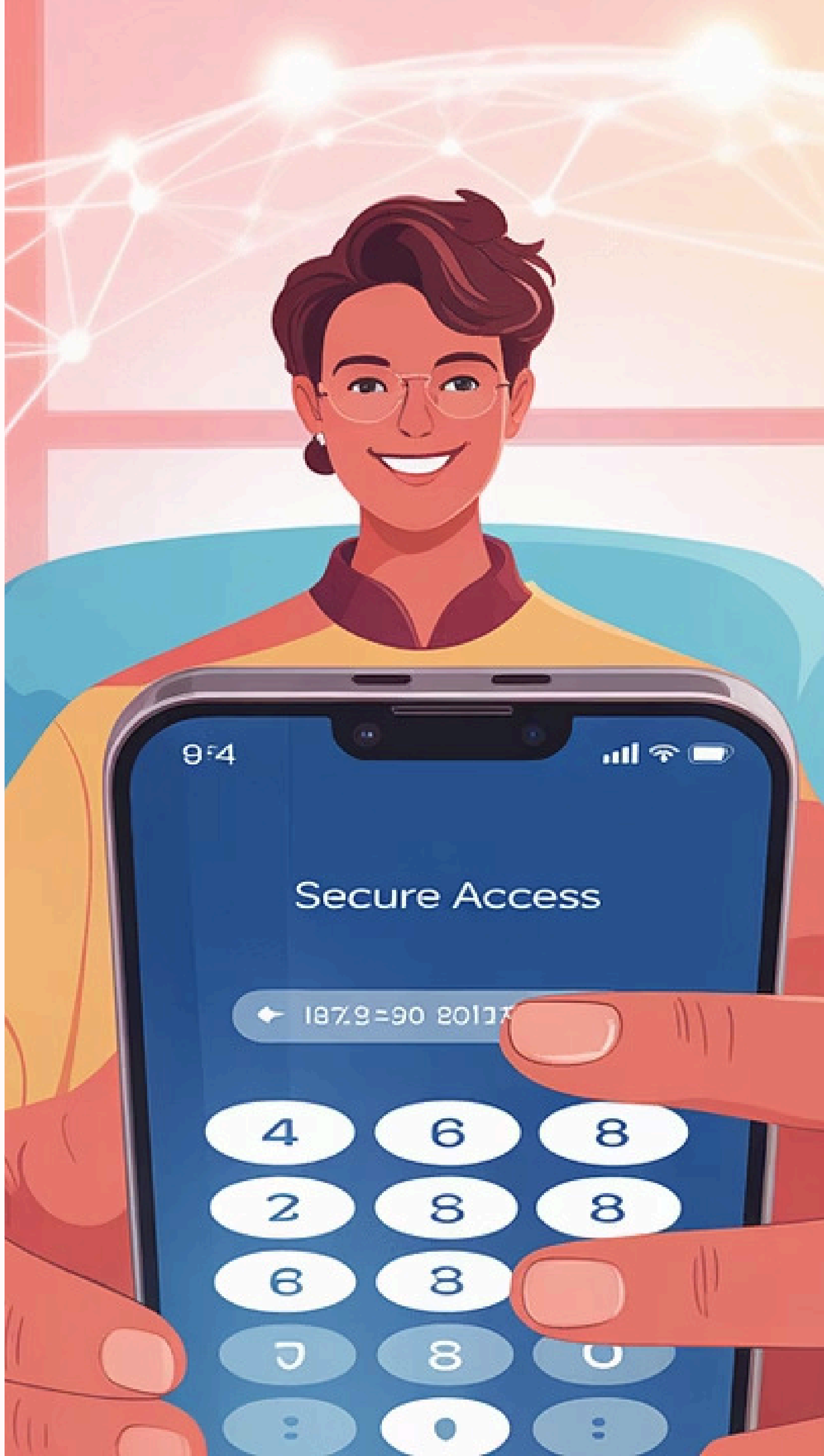
Additional security layer requiring a second verification method

- Virtual MFA devices (smartphone apps like Google Authenticator)
- Hardware MFA tokens (YubiKey, Gemalto)
- SMS text message verification (less secure but available)

Temporary Security Credentials

Short-lived credentials for reduced risk exposure

- AWS Security Token Service (STS) for temporary access
- Automatic rotation of credentials
- Configurable expiration periods



Identity Federation and Cross-Account Access

Identity Federation Solutions

SAML 2.0 Federation

Integrate with enterprise identity providers like Active Directory, Okta, or Ping Identity

Web Identity Federation

Authenticate via Google, Facebook, Amazon, or any OpenID Connect compatible provider

AWS SSO

Centrally manage access to multiple AWS accounts and business applications

Cross-Account Access

AWS enables secure access patterns across multiple accounts through:

- Cross-account IAM roles with defined trust relationships
- Resource-based policies allowing specific external account access
- AWS Organizations for hierarchical account management

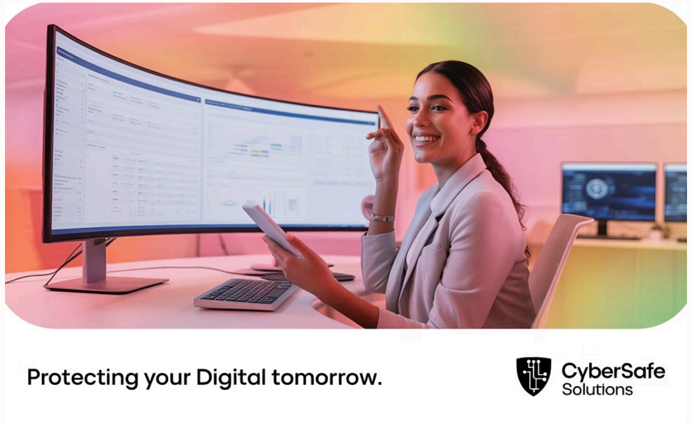
Compliance, Auditing, and Monitoring

Comprehensive Logging

AWS CloudTrail automatically records all API calls, providing detailed event history of actions taken in your AWS account. This includes who performed what action, when it occurred, and from which IP address.

Regulatory Compliance

IAM helps meet regulatory requirements for HIPAA, PCI DSS, SOC, and FedRAMP through granular access controls, separation of duties, and comprehensive audit trails.



Access Analyzer

IAM Access Analyzer identifies resources shared with external entities, helping prevent unintended access and maintaining the principle of least privilege across your organization.

Best Practices in AWS Access Management

Implement Least Privilege

Grant only the permissions required to perform specific tasks, starting with minimal access and expanding as needed.

Use IAM Roles for Applications

Never embed access keys in application code or instances. Instead, use IAM roles for EC2 and other AWS services.

Enforce MFA

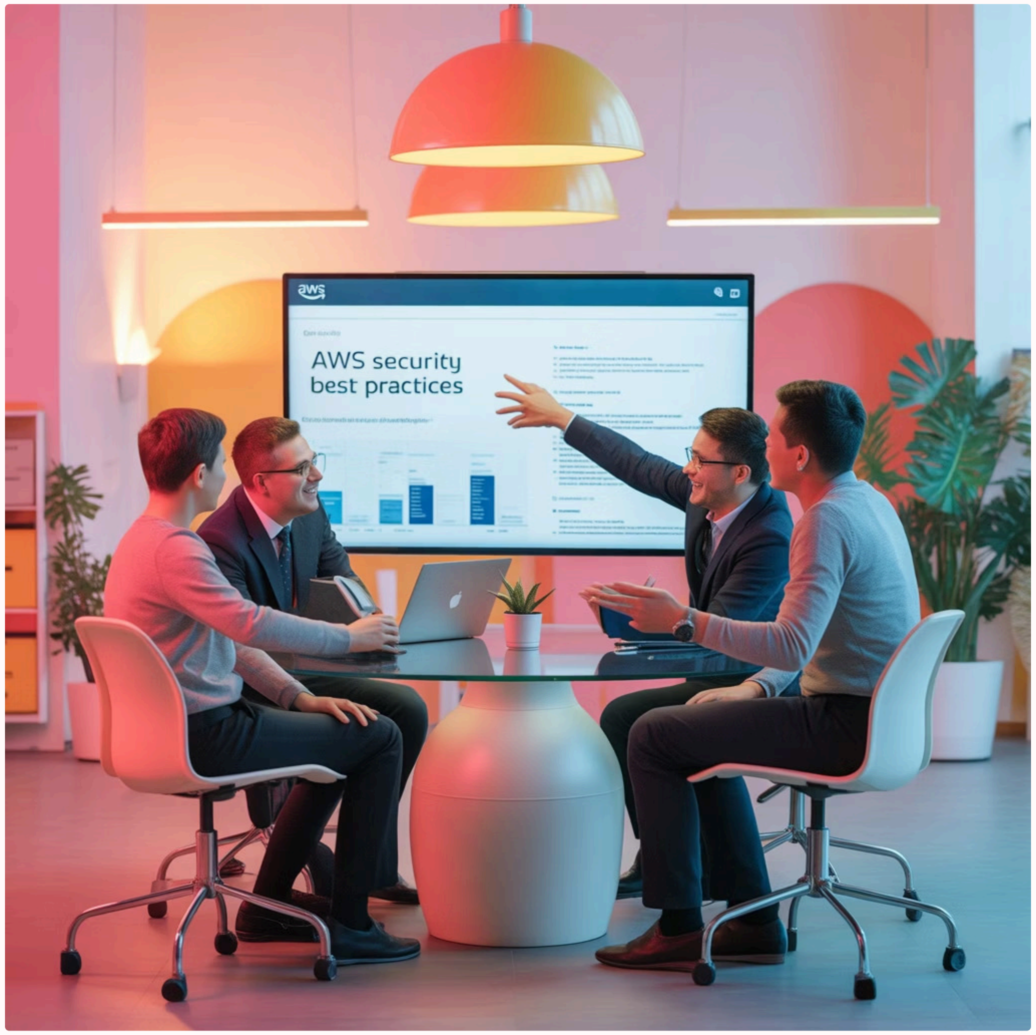
Require multi-factor authentication for all users, especially those with elevated privileges or access to sensitive data.

Regular Audits

Periodically review access patterns, remove unused credentials, and verify that policies align with current security requirements.

Learn More

Practice Exams



Key Security Considerations

- Rotate credentials regularly (at least every 90 days)
- Use AWS Organizations with Service Control Policies to enforce guardrails
- Implement a strong password policy with minimum complexity requirements
- Monitor and respond to AWS Security Hub findings
- Use IAM Access Advisor to identify and remove unused permissions