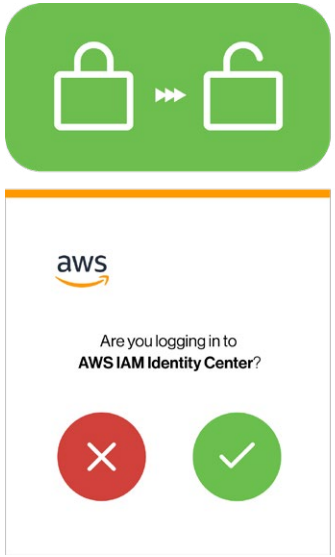
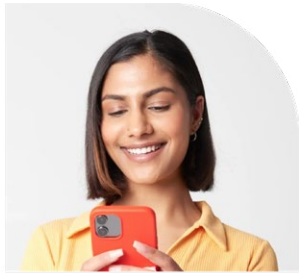
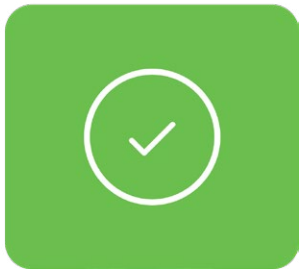
Seamless zero trust access for the AWS cloud

As businesses progressively embrace cloud platforms, it's imperative to protect them from unauthorized access, data breaches, and cyberattacks. Cisco Duo has partnered with Amazon Web Services (AWS) to establish an effective zero trust security framework for AWS customers, prioritizing productivity and business scalability while safeguarding data and access against potential security risks.







- Multi-factor Authentication
- Single Sign-On
- Passwordless Authentication
- Device Posture Policies
- Trusted Endpoints
- Risk-Based Authentication

and more...

Prevent unauthorized access

While cloud services offer advantages such as scalability and flexibility, they're also a target for cybercriminals. To bolster the security of the AWS infrastructure and to easily implement a zero trust architecture for secure access, Duo offers a comprehensive access management solution. This includes a robust foundation built on strong multi-factor authentication (MFA) and encompasses single sign-on (SSO), passwordless authentication, device posture policies, trusted endpoints, risk-based authentication (RBA), and more, all aimed at mitigating potential security concerns.

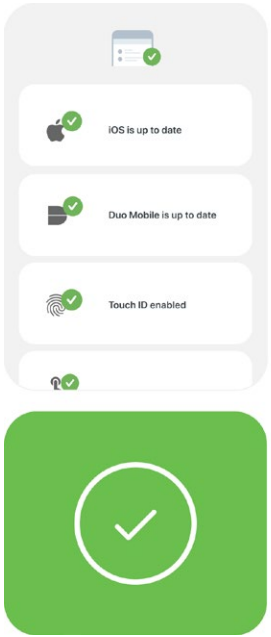
Prevent cybersecurity attacks and data breaches

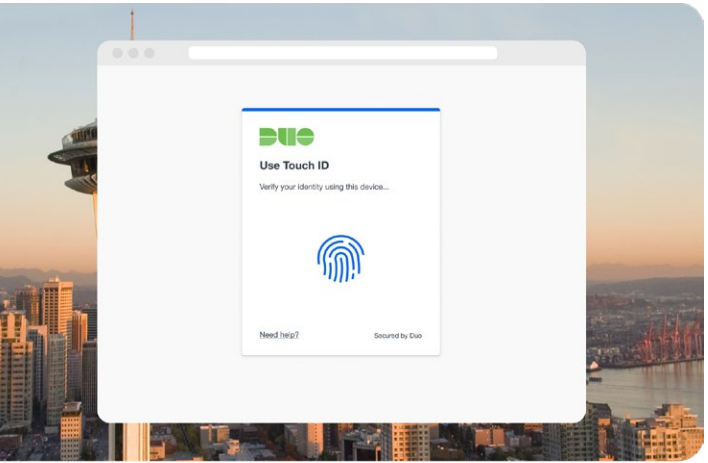
Duo MFA for AWS Directory Services

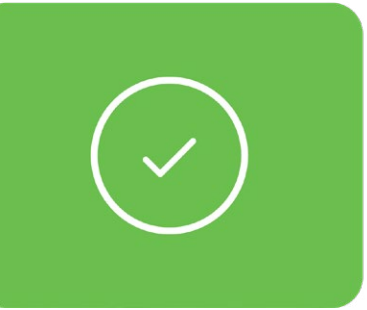
Secure MFA logins to the AWS Directory Services in minutes with Cisco Duo using the Duo Quick Start guide.

Once deployed, Duo MFA provides a secure, fast, and non-disruptive way for IT admins to log into AWS cloud using Duo Mobile app. Adaptive controls strengthen user authentication by evaluating changing contexts.

- Admins can bulk deploy users and provision them using the Duo Admin Dashboard.
- Additionally, granular access policies can be set for groups of users.







Duo SSO and passwordless for AWS apps

Duo SSO and passwordless pair with AWS IAM and AWS IAM Identity Center, establishing trust in users and devices before granting access to applications. Contextual factors allow access based on the level of risk each login poses to the organization.

Duo is also compatible with some AWS apps, including:

- AWS IAM Identity Center
- AWS IAM
- Amazon Connect
- AWS Verified Access
- Amazon Managed Grafana
- Amazon Redshift
- AWS Client VPN

Admins' burden on password management is significantly reduced when end users adopt SSO and passwordless methods with a combination of self-service features.

Duo Desktop for AWS Workspaces (private preview)

Duo Desktop evaluates the posture of any device attempting access to virtual desktops using AWS Workspaces. Based on the security criteria you select, Duo Desktop allows or blocks device access to prevent non-compliant device access.

- Granular controls are available to IT admins to create policies for managed or unmanaged devices.
- Reporting and auditing this data can provide deeper insights and help investigate various security events.

Learn more

Duo Essentials on AWS marketplace

Duo Advantage on AWS marketplace

Duo Premier on AWS marketplace