Duo Single Sign-On

Simple, secure application access for the workforce

Today, organizations on average use 100s of workforce applications. The movement to cloud-based apps can increase organizational agility and lower costs, but it can also result in a lot of usernames and passwords, which can be frustrating for employees and taxing on IT teams.

By enabling employees to access multiple apps with just a single username and password, Duo Single Sign-On (SSO) provides an easy and consistent login experience for any application, whether it is on-premises or cloud-based.

Duo Single Sign-On is a cloud-hosted service that enables simple, secure application access for end-users and is easy to set-up, deploy and manage for admins. When paired with the world's most flexible MFA or passwordless authentication and device trust, Duo SSO enables and protects access to all platforms and applications from any user, device, and location.

Why Duo SSO?

Security Focus:

• Reduce risk of data breaches by reducing user reliance on multiple passwords

• Strengthen security by customizing access policies per application, providing just the right level of access for each user

• Enforce MFA for users accessing apps via Duo SSO to help your organization adhere to regulatory compliance requirements (e.g. PCI DSS, HIPAA, etc.) for verification of users

• Pair cloud-based SSO with either Duo's industry-leading Multi-Factor Authentication (MFA), deployed by over 40,000 customers globally, or with Duo Passwordless Authentication

• Use Duo's built in security for device health checks, remediation, location-based controls, device trust and endpoint visibility

Ease of Use and Rapid Time to Value:

• Roll out security enterprise-wide in hours, with low-touch deployment and minimal maintenance

• Provide a seamless login experience by giving users access to approved apps, helpful links, and the ability to self-manage and enroll authentication devices through Duo's web-based portal, Duo Central

• Decrease administrative burden by reducing number of login credentials to be provisioned and managed while enabling multiple end-user self-service capabilities

• Help IT and helpdesk teams save time and costs associated with onboarding new users to applications, password resets, device management and more

• Pave the way for modern approaches to access management such as passwordless authentication

• Centrally manage policies and view overall security status with Duo's Admin Panel: flag risky devices and use policy controls to limit access based on device and user trust

• Use easy to understand online documentation and strong support

**Comprehensive:**

• Protect access to any application whether on-premises, in hybrid, or multi-cloud environments

• Integrate Duo SSO with existing federation and identity providers or IdPs (e.g. Microsoft, Okta, Ping), allowing you to secure application access in the way that works best for your business

- Secure access to platforms and applications, for different user groups and types of devices

- Enable users to access applications from the office, on the road, at home or elsewhere

- Adopt passwordless authentication with platform biometrics, security keys, or Duo Mobile as authenticators, using the easiest to deploy and manage passwordless SSO solution on the market

Duo SSO verifies the user's credentials and prompts for MFA or Passwordless Authentication before permitting access to a requested application.
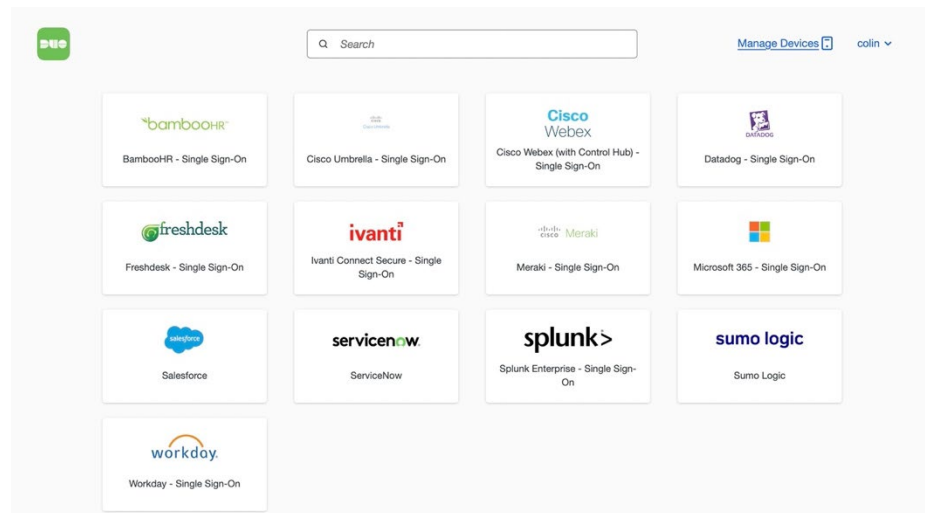
Users get convenient access to their apps and other helpful links and can self-manage and enroll authentication devices from Duo Central.

How Duo SSO works

Duo SSO is a cloud-hosted product that layers Duo's strong authentication and flexible policy engine on top of an application's login using the Security Assertion Markup Language (SAML) 2.0 or OpenID Connect (OIDC) authentication standards.

With Duo SSO as your Identity Provider (IdP), authenticating your users is easier than ever before. You can use your existing on-premises Active Directory (AD) or any SAML 2.0 (IdP) provider, and Duo will prompt for two-factor authentication before permitting access to your service provider application.

Duo provides SAML connectors for a variety of enterprise cloud applications including Amazon Web Services, Salesforce, Workday and others. In addition, Duo SSO features a generic connector with that enables the use of custom SAML "metadata" to connect to any app that supports the SAML 2.0 standard.

Duo SSO allows organizations to add OIDC Relying Party applications into the platform. We support commonly used OIDC and OAuth 2.0 AuthN and AuthZ flows: authorization code (in public preview), client credentials, refresh tokens, and authorization code with PKCE.

Additionally, Duo Central is a web based portal hosted by Duo that acts as a single place for end users to conveniently access all their applications and other helpful links as well as self-manage and enroll their authentication devices.

Pricing

	Duo Free	Duo MFA	Duo Access	Duo Beyond
Multi-Factor Authentication	✔	✔	✔	✔
Unlimited application integrations		✔	✔	✔
User Self-Enrollment and Self-Management		✔	✔	✔
Passwordless Authentication to SSO Applications (Duo SSO, third-party SSO)		✔	✔	✔
Cloud-based Single Sign-On (SSO) for SAML 2.0 and OIDC apps		✔	✔	✔
Easy Application Access with Duo Central		✔	✔	✔
Policy Enforcement		✔	✔	✔
Adaptive Authentication			✔	✔
Device Visibility			✔	✔
Device Remediation			✔	✔
Device Health App			✔	✔
Trusted Endpoints				✔
VPN-less Remote Access				✔
Monthly Price	Free for up to 10 users	$3/User	$6/User	$9/User

To learn how to implement Duo SSO, visit: duo.com/docs/sso.

For more information about Duo product capabilities, please visit: duo.com/product.

Summary

Having smooth and fast access to work applications and internal sites, without the temptation of using the same password or the difficulty of remembering multiple passwords, is essential. A single sign-on solution like Duo SSO can make this happen by providing a seamless user experience backed by strong security. Thousands of companies worldwide have already benefited from Duo SSO,
now it's your turn.