



Access Management by Duo

Strong security that powers
high productivity

Duo protects against breaches with a leading access management solution that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. For any organization concerned about being breached and needs a solution fast, Duo quickly enables strong security while also improving user productivity.

Defend your organization against compromised credentials, risky devices, and unwanted access to applications and data. Duo helps you ensure only the right users on trusted devices gain access to permitted applications under the right conditions by dynamically evaluating risk levels and adjusting requirements based on the current situation.

Duo Editions

From setting up MFA for just a few users to securing your entire workforce with a comprehensive access management solution, Duo meets organizations at their secure access needs.

Duo Essentials – \$3/user/month

Get everything needed to secure access and boost user productivity.

Duo Essentials is a full-featured access management solution that includes strong MFA, Passwordless, Single Sign-On (SSO) and Trusted Endpoints verification for every organization.

- **MFA with Verified Duo Push:** combat MFA fatigue attacks and use **FIDO2 authenticators** such as security keys and platform biometrics for phishing-resistant MFA.
- **Duo Single Sign-On (SSO) with Duo Central:** enable a consistent user login workflow across all applications and easy application access.
- **Passwordless Authentication:** enable secure, seamless access to applications with Duo Mobile, FIDO2 security keys and device biometrics.
- **Trusted Endpoints:** block access from unknown devices and only allow trusted devices to gain access to resources.
- Integrate with **Cisco Secure Endpoint:** prevent infected devices from accessing resources.
- **Access Policies:** assign and enforce authentication globally or per user group.
- **Authorized Networks:** apply policy to enable access only from authorized networks.
- **Visibility:** view dashboard of all devices accessing applications with device insight



Duo Advantage - \$6/user/month

Upgrade to stronger security and higher user productivity with full device trust, additional visibility into device health status, machine learning-driven attack detection and risk-based authentication.

Duo Advantage is a management suite that maximizes security and visibility to address constant changes in risk levels and the need for rapid security incident detection and detailed visibility.

Includes everything in Duo Essentials, plus:

- **Risk-Based Authentication:** adjust authentication requirements in real-time based on user and device risk.
- **Device Health:** perform checks for updated operating systems, browsers and compliance with security policies.
- **Adaptive Access policies:** assign and enforce adaptive access policies globally or per application, or per user group (based on user's location, device health or network).
- **Duo Trust Monitor:** machine learning that detects potential attacks in progress, and surfaces suspicious device registrations, access attempts and activity to aid in security investigations.
- **Duo Admin Panel:** full-featured dashboards and custom reports for compliance audits and ease of administrative management, with deeper visibility into devices.

Duo Premier - \$9/user/month

Expand protection and effortless access to cloud and on-premises resources and private applications.

Duo Premier is a complete access management solution that addresses user and device risk for every application and expands protection and ease of access to on-premises and private resources.

Includes everything in Duo Essentials and Advantage, plus:

- **Duo Network Gateway:** provide end-users with **VPN-less remote access** to private applications hosted on-premises or in multi-cloud environments while enforcing zero trust security principles. Enable secure, seamless SSO access to internal web applications (HTTPS) and servers via SSH, RDP and SMB.
- **Endpoint Protection check:** Limit device access to applications based on presence of endpoint protection product (CrowdStrike, SentinelOne, Cisco Secure Endpoint, etc.)



User Authentication

Ensure users are who they say they are

Duo Essentials

Duo Advantage

Duo Premier

MFA

MFA with security keys, FIDO2, OTP, phone callback¹, SMS & hardware tokens



Multi-Factor Authentication with Duo Push for iOS and Android



Unlimited application integrations



User self-enrollment & self-management



Telephony credits: 100 credits/user/year



Push Phishing Protection

Customizable number-matching with Verified Duo Push MFA



Enforce utilization of phishing-resistant factors



Immediate alert of suspicious logins



Passwordless

Passwordless Authentication to SSO Applications (Duo SSO, third-party SSO)



Duo Mobile as Passwordless authenticator



Threat Detection

Surface anomalous and risky logins with Machine Learning for detection of potential attacks in progress (Trust Monitor)



Detect new registration of authentication devices





Device Trust

Ensure only known and healthy devices can access resources

Duo Essentials

Duo Advantage

Duo Premier

Trusted Endpoints

Allow only managed and registered devices to access applications



Enforce trust on BYOD and 3rd party devices through device registration



Limit device access to applications based on enrollment in endpoint management systems such as LANDesk, JAMF, Microsoft Intune



Limit mobile access to applications based on enrollment in mobile device management systems such as AirWatch, MobileIron, Microsoft Intune



Integrates with Cisco Secure Endpoint to block compromised devices



Device Health

Enforce device trust policies based on security health of laptops and desktops (out-of-date software, encryption, firewall, etc.)



Enforce device trust policies based on security health of mobile devices (encryption, tampered, screen lock, biometrics)



Notify users when and how to self-remediate their devices without helpdesk intervention



Limit device access to applications based on presence of endpoint protection product (CrowdStrike, SentinelOne, Cisco Secure Endpoint, etc.)



Visibility

Dashboard of all devices accessing applications (Device Insight)



Visibility into security health of mobile, laptops and desktops – checks such as updated operating systems, browsers and compliance with security policies (Duo Device Health)



Full-featured dashboards, authentication logs, and custom reports for compliance audits and ease of administrative management





Authentication and Access Policies

Increase security and visibility by enforcing adaptive access policies and dynamic risk-based policies

Duo Essentials

Duo Advantage

Duo Premier

Risk-Based Authentication

Dynamically adjust authentication requirements in real time based on risk signals



Uses an array of accurate signals, such as Wi-Fi fingerprinting, to determine risk level and enforce risk-based policies while preserving user privacy



Enable longer sessions and only require re-authentication when risk signals change



Adaptive Access Policies

Assign and enforce authentication globally or per user group



Enforce policies based on authorized networks



Assign and enforce security policies per application



Block authentication attempts from anonymous networks like Tor, proxies, and VPNs



Enforce policies based on device health status





Enable Access - Single Sign-On (SSO) and Remote Access

Make it easy and safe for users to access what they need and stay productive

Duo Essentials

Duo Advantage

Duo Premier

Single Sign-On (SSO)

Cloud-based SSO for all SAML 2.0 and Open ID Connect (OIDC) applications



Unlimited application integrations



Easy application access and user device self-enroll/management with Duo Central



Passwordless login to Duo Central



Integrates with existing on-premises or cloud federation and identity providers or IdPs (e.g., Microsoft, Okta, Ping)



Supports commonly used OIDC and OAuth 2.0 AuthN and AuthZ flows: authorization code, client credentials, refresh tokens, and authorization code with PKCE



Remote Access with Duo Network Gateway

VPN-less remote access to private applications (hosted on-premises or multi-cloud environments)



Secure access to internal web applications (HTTPS) and internal servers via SSH, RDP and SMB



Secure remote access to applications hosted in Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP)





Support

Duo Basic Support

Included with purchase of any Duo subscription

- Access to support and troubleshooting via phone, online tools, and web case submission
- 9-5 ET, 9-5 PT, M-F. 24x7x365 support for critical issues (Premium available)
- Access to <https://duo.com/support> with helpful technical and general information on Duo products, as well as access to Duo's online community and documentation

Duo Premium Support (Duo Care)

Available to purchase with every edition of Duo based on the total number of user licenses

- Strategic support from an assigned Customer Success Manager
- Technical support and response from an assigned Customer Solutions Engineer
- 24x7 x 365 support
- Priority Ticket SLA
- VIP Support Line - extended Duo support access 18 hours per day (local time), 5 days a week to assist by a VIP support line
- Duo Quick Start for organizations that are new to Duo and are ready to focus on deployment for up to 3 applications and a user population under 1,500

Pricing

	Duo Essentials	Duo Advantage	Duo Premier
Price Per Month	\$3/user	\$6/user	\$9/user

Support

Duo Basic Support is included with any purchase of Duo.

For Premium Duo Care support and Duo Quick Start, contact your Sales representative or go to <https://duo.com/about/contact>

Summary

Only Duo provides advanced security features that protect the broadest variety of environments, users, devices and applications in one seamless solution that is easy to deploy, simple to use and cost-effective.

Find out yourself by [trying Duo free for 30 days.](#)

Start your free 30-day trial at duo.com/trial.

