# Continuous Identity Security by Cisco Duo

## Stop identity-based threats and boost workforce productivity.

Duo's Continuous Identity Security solution adds a powerful security layer for any identity infrastructure and provides the best-in-class access experience across all users, devices, and applications. IT and security teams benefit from reducing coverage gaps in heterogeneous environments and swift responses to detected threats. End users benefit from fewer authentication interruptions for an enhanced productivity experience in trusted scenarios.

Powered by Cisco Identity Intelligence, Duo provides deep, cross-platform identity visibility and uses AI to assess and dynamically respond to identity-related threats before, during, and after login. Detect session hijacking, inactive account probing, MFA flood, and other sophisticated identity threats using AI-based detection logic. And automate response by incorporating identity risk and context into Duo's dynamic risk-based authentication policies.

## Duo Editions

From setting up MFA for just a few users to securing your entire workforce Duo provides organizations with simple and effective tools to secure their workforce identity perimeter.

### Duo Essentials

Get everything needed to secure your identity perimeter and boost user productivity. Duo Essentials is a strong identity security solution that includes:

- 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 work low 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

Upgrade to Continuous Identity Security with Duo Advantage. Get cross-platform identity visibility and threat response capabilities, and a seamless access experience that is dynamically informed by risk – before, during, and after login.

Duo Advantage provides complete visibility of identity security posture (ISPM), device security posture, AI-based identity threat detection and response (ITDR), dynamic risk-based authentication and a seamless login experience that minimizes repeated authentications.

### Includes everything in Duo Essentials, plus:

- Cisco Identity Intelligence: Identify, detect, protect, and respond to identity-based threats by gaining multi-vendor visibility across identity sources and incorporate identity context into Duo's risk-based authentication policies.
- Duo Passport: authenticate once on a trusted device and get uninterrupted access to permitted applications across browsers and thick clients, minimizing repeated authentication requests.
- Risk-Based Authentication: adjust authentication requirements in real time based on risk signals.
- Device Health: perform checks for updated operating systems, browsers, and compliance with security policies.
- Adaptive Access Policies: enforce adaptive access policies per application based on user's location, device health or network.
- Duo Trust Monitor: machine learning that detects potential attacks in progress, and surfaces suspicious events.
- Visibility and Reporting: full-featured dashboards and custom reports for compliance audits and ease of administrative management, with deeper visibility into devices.

## Duo Premier

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

Duo Premier is a complete identity security and 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.).

CISCO DUO

# User Authentication

Ensure users are who they say they are

| | Duo Essentials | Duo Advantage | Duo Premier |
|---|---|---|---|
| **MFA** | | | |
| MFA with security keys, FIDO2, OTP, phone callback[1], SMS and 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 | ✓ | ✓ | ✓ |
| **Identity Posture and Threat Detection** | | | |
| Gain visibility across identity sources into MFA usage, admin controls, inactive or dormant accounts, excessive permission, and more (Cisco Identity Intelligence) | | ✓ | ✓ |
| AI-based detection for identity-based threats such as session hijacking, MFA flood, and more (Cisco Identity Intelligence) | | ✓ | ✓ |
| Surface anomalous and risky logins with Machine Learning for detection of potential attacks in progress (Trust Monitor) | | ✓ | ✓ |
| Detect new registration of authentication devices | | ✓ | ✓ |
| **Duo Passport** | | | |
| Reduce the number of times users need to authenticate without compromising security | | ✓ | ✓ |

CISCO DUO

# 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, Meraki Systems Manager | ✓ | ✓ | ✓ |
| 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 | | ✓ | ✓ |

CISCO DUO

## 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 | | ✓ | ✓ |

CISCO DUO

## 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) | | | ✓ |