
# STONE SOLUTIONS

## Multi-factor Authentification

# Cisco Duo at a glance

stone
A CONVERGE COMPANY

CONVERGE
TECHNOLOGY SOLUTIONS

cisco Meraki

Multi-factor Authentification

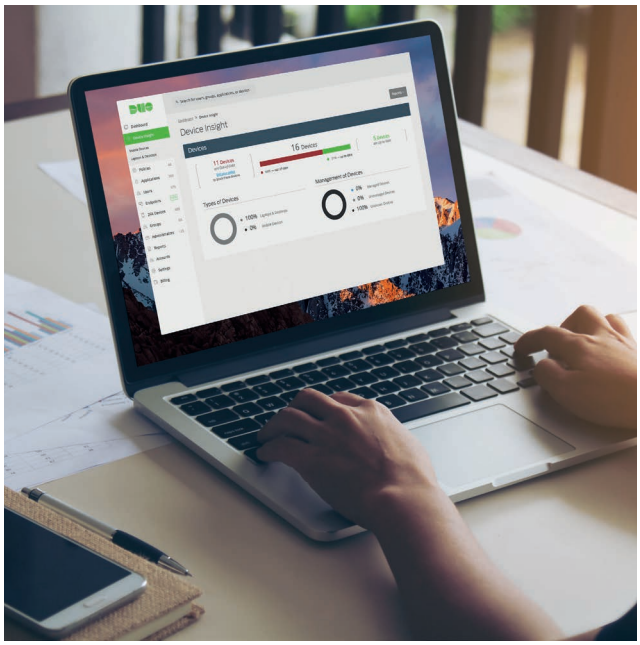
# Trusted Access

## Duo ensures only trusted users and trusted devices can access every application.

**Duo's Trusted Access platform is a holistic security solution that reduces your risk of a data breach caused by compromised credentials, known vulnerabilities and/or exploits.**

Using multi-factor authentication, Duo verifies your users' identities. Then, Duo checks your users' devices for out-of-date software, missing security features and certificates, enabling you to enforce device access policies to block any risky or untrusted devices.

Finally, Duo grants your users access to only the applications you want them to access, while giving them simplified access to their on-premises and cloud applications with secure single sign-on.



# Trusted Users

## Verify your users' identities with multi-factor authentication:

> Easy-to-use authentication app, Duo Mobile allows for easy one-tap login via Duo Push

> Other methods include U2F, SMS passcodes, mobile OTP, phone callback & security tokens

> Works with various identity providers (AD, OneLogin, Okta, Ping) through multiple authentication protocols (LDAP, SAML, OIDC)

> Easily provision users, and automate management with Admin APIs

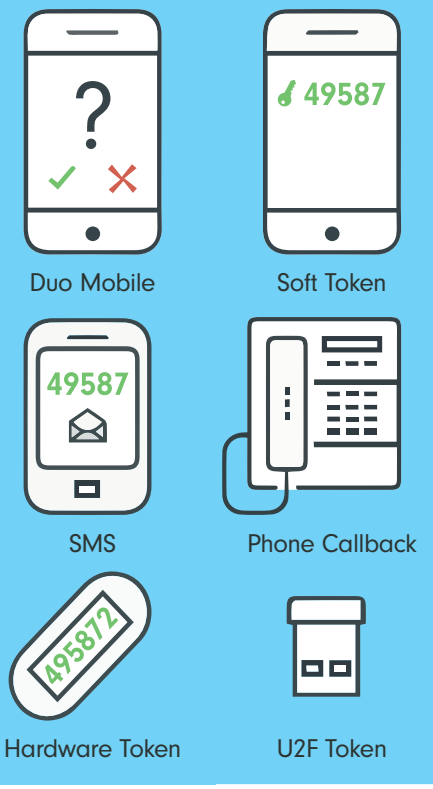
> Vulnerability assessments using Duo's phishing simulation tool

## Enforce user access policies:

> Block logins based on IP or countries

> Block users on anonymous networks, like Tor

## Authentication methods to support every user:



cisco Meraki

stone A CONVERGE COMPANY

## Multi-factor Authentification

cisco DUO

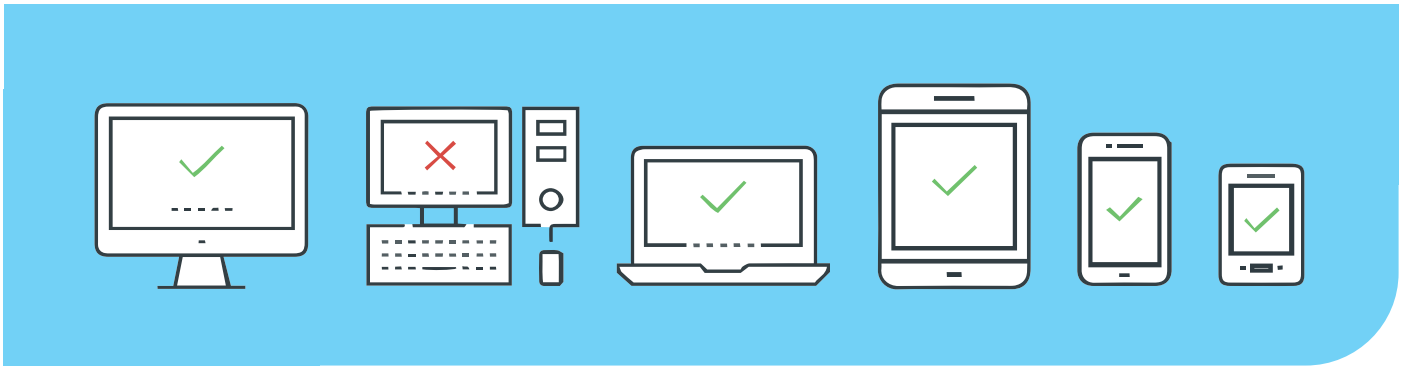
# Trusted Devices

### Check the security health of all your users' devices, including:

> Out-of-date operating systems, browsers or plugins
> Enabled security features, like screen lock
> Rooted or jailbroken status
> Trusted or not based on certificates

### Enforce device access policies:

> For corporate-owned vs. personal devices
> Control what devices can access apps based on device certificates
> Block, notify and restrict access of users with risky devices
> Prompt users to update their own devices



# Every Application

### Secure access to any application:

> Integrate with on-premises apps like RDP, SSH, UNIX & more
> Secure VPNs & remote access gateways like Cisco, Juniper, etc.
> Native support for protecting all cloud apps like Office 365, Salesforce, AWS & more
> Protect federated cloud apps
> Allows users to connect to on-premises web apps without a VPN

### Enforce application access policies:

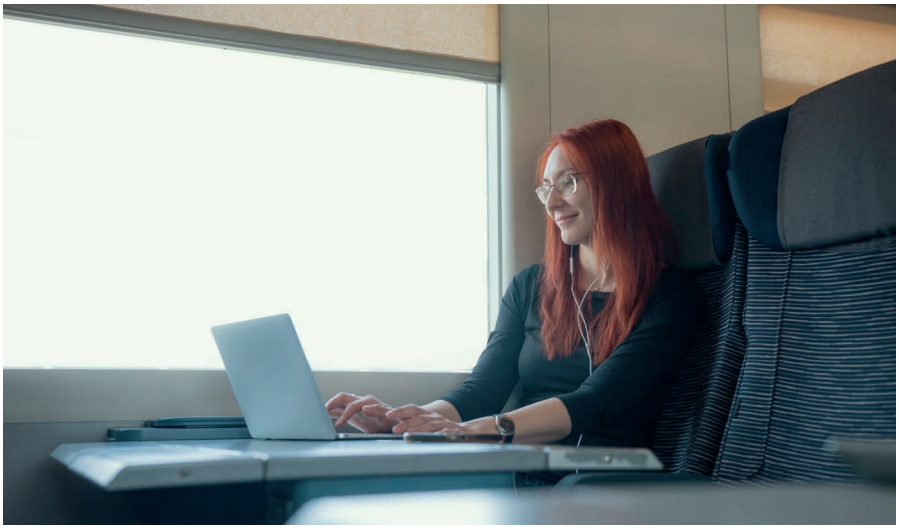
> Control which internal apps are accessible by remote users
> Provide a single web portal to access on-premises and cloud-based applications with Duo's secure single sign-on (SSO)

### Protect every application:

box, salesforce, Office 365
zendesk, Epic, amazon web services
workday, Dropbox, Outlook
cisco, Google apps, vmware
slack, JUNIPER NETWORKS, CITRIX

and many more...

cisco Meraki



Duo delivers simple, secure access to all applications – for any user, from any device, from anywhere.

## MFA, Access and Beyond

The rise of mobile workers and the dawn of cloud require organizations to provide users secure and reliable access to applications from any device on any network. And that security should be simple to deploy and seamless to use. Duo's Unified Access Security (UAS) solution offers three unique editions based on your business' secure access needs:

### Duo MFA

Duo's multi-factor authentication (MFA) establishes trust in users' identities and protects every user with a reliable, easy-to-use experience. Traditional 2FA can take months to deploy, requires professional services, and drives up total cost of ownership with ongoing management. Duo MFA delivers speed-tosecurity and lower costs with a faster, cloud-based deployment, as well as simplified authentication for users and admins with quick, push notification based approvals with support for smartphones, smartwatches and U2F tokens.

Duo MFA is easy to deploy, scales up to meet the needs of even the most diverse user base, and delivers device insights summarizing the security posture of your devices. Duo MFA also comes with single sign-on (SSO) for cloud applications. With SSO, users can find and access all their cloud applications from a single portal.

### Duo Access

Duo Access takes everything in Duo MFA and supercharges it. It delivers Unified Device Visibility, an admin dashboard that includes all corporate-owned and bring your own devices (BYOD) in your environment.

Duo Access packs intelligence to check devices for secure, up-to-date software, enabled security settings and location and network data. You can set policies that allow or restrict access to applications based on individual users and groups, location, network data, device security posture and other contextual information.

Duo Access gives admins the ability to define the specific conditions under which users can access applications, to secure BYOD environments and to encourage users to update their device software. It's complete visibility without the need for agents.

### Duo Beyond

Based on the zero-trust security model, Duo Beyond empowers you to base application access decisions on the trust established in user identities and the trustworthiness of their devices, instead of the networks from where access originates. It combines everything available in Duo Access plus the ability to differentiate between corporate and employee-owned devices and control which devices can access which applications based on the trustworthiness of the device and the identity of the user requesting access.

Duo Beyond allows admins to publish internal applications on the internet. Users are able to access on-premises and cloud applications from a single dashboard. Admins can develop specific controls for BYO devices to ensure only secure and trusted devices can access internal and cloud applications.