Cisco Duo Security NEW

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED

Secure Access for Everyone, from Any Device, Anywhere

The **Duo Security** (now part of Cisco) is a cloud-based security platform that protects access to all applications, for any user and device, from anywhere. Duo is designed to be both easy to use and deploy while providing complete endpoint visibility and control.
Duo verifies users' identities with strong multi-factor authentication (MFA). Paired with deep insights into your users' devices, Duo gives you the policies and control you need to limit access based on endpoint or user risk. Users get a consistent login experience with Duo's single sign-on (SSO) that delivers centralized access to both on-premises and cloud applications.
With Duo, you can protect against compromised credentials and risky devices, as well as unwanted access to your applications and data. This combination of user and device trust builds a strong foundation for a zero-trust security model.
Duo helps organizations:

- Reduce compromised credential and device risk
- Reduce time to security
- Increase visibility and granular control
- Save time and costs, centralize access security

Highlights

Solutions that Duo provides:

Multi-Factor Authentication (MFA)

Confirm user identities in a snap.

Device Trust

Monitor the health of managed and unmanaged devices.

Adaptive Access Policies

Set adaptive security policies tailored for your business.

Remote Access

Secure remote access without a device agent.

Single Sign-On (SSO)

Provide security-backed, user-friendly SSO.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Duo Security NEW

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED

Cisco Duo Edition Comparison

		Duo Free	Duo MFA	Duo Access	Duo Beyond
Multi-Factor Authentication (MFA)	MFA with Duo Push (Duo Mobile App) for iOS and Android	✓	✓	✓	✓
	MFA with security keys (Duo Mobile App, SMS, phone callback, hardware token), biometrics (U2F, WebAuthN), etc.	✓	✓	✓	✓
	Telephony credits (100 credits/user/year)*1		✓	✓	✓
	User self-enrollment & self-management		✓	✓	✓
Device Trust	A dashboard of all devices accessing applications		✓	✓	✓
	Monitor and identify risky devices			✓	✓
	Visibility into security health of laptops and desktops (Duo Device Health application)			✓	✓
	Visibility into security health of mobile devices			✓	✓
	Identify corporate-owned versus BYOD laptops and desktops				✓
	Identify corporate-owned versus BYOD mobile devices				✓
	Identify if a third-party agent is enabled on the device (e.g., anti-virus, anti-malware)				✓
Adaptive Access Policies	Assign and enforce security policies globally or per application		✓	✓	✓
	Enforce policies based on authorized networks		✓	✓	✓
	Enforce policies based on user's location			✓	✓
	Assign and enforce security policies per user group			✓	✓
	Block Tor and anonymous networks			✓	✓
	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, etc.)			✓	✓
	Notify users to remediate their devices			✓	✓
	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 MDMs (AirWatch, MobileIron, Microsoft Intune)				✓
Remote Access	Secure access to internal company web applications (Duo Network Gateway)				✓
	Secure access to specific internal servers via SSH (Duo Network Gateway)				✓
	Secure remote access to applications hosted in AWS, Azure, and GCP (Duo Network Gateway)				✓
Single Sign-On (SSO)	Unlimited application integrations	✓	✓	✓	✓
	SSO for all cloud applications		✓	✓	✓

*1 Paid accounts are issued telephony credits yearly, and may purchase extra telephony credits as needed.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Duo Security NEW

Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED

Cisco Duo MFA License

Product SKU*1	Description
DUO-MFA	Duo MFA per User License

*1 DUO-SUB is required in CCW. See Ordering Guide for details.

Cisco Duo Access License

Product SKU*1	Description
DUO-ACCESS	Duo Access per User License

*1 DUO-SUB is required in CCW. See Ordering Guide for details.

Cisco Duo Beyond License

Product SKU*1	Description
DUO-BEYOND	Duo Beyond per User License

*1 DUO-SUB is required in CCW. See Ordering Guide for details.

Cisco Duo Hardware Tokens

Product SKU	Description
DUO-TOKEN	Duo Hardware Tokens (10 Pack)

Cisco Duo Technical Support

Product SKU*1	Description
SVS-DUO-SUP-B	Duo Basic Support*2
SVS-DUO-SUP-P	Duo Premium Support (Duo Care)

*1 DUO-SUB is required in CCW. See Ordering Guide for details.
*2 Included with the purchase of Duo subscription.

Ordering and Licensing Guide

Duo Security (now part of Cisco) is licensed on a subscription basis. Each end customer has only one subscription, though each subscription may comprise multiple products. Subscriptions are available for standard term lengths of 12-60 months. At time of ordering, the subscription is set to auto-renew as default; however, auto-renew can be turned off without triggering the deal to become nonstandard. If the order is booked as auto-renew, the subscription will be renewed automatically for an additional 12-month term following the completion of the initial term. If the removal of auto-renew after purchase is necessary, the auto-renewal option must be canceled 60 days or more before the start date of the new term. Mid-term cancellations of subscriptions for credit are not allowed.
The user-based license follows a tiered-pricing model: pricing depends on the number of user licenses purchased. Sales and partner representatives should determine the correct sizing for each customer deployment so that the appropriate user count is selected. Cisco Commerce Workspace (CCW) will dynamically determine the correct price associated with the user count entered.

Cisco Technical Services for Duo

Cisco Duo Basic Support provides:

- Access to support and troubleshooting via phone, online tools, and web case submission.
- Cisco Duo support access 9 hours per day (local time), 5 days per week to assist by telephone, web case submission and online tools with application use and troubleshooting issues.
- Access to https://duo.com/support. The support site provides customers with helpful technical and general information on Duo products, as well as access to Duo's online community and documentation.

Cisco Duo Premium Support provides:

- Strategic support from an assigned Customer Success Manager
- Technical support and response from an assigned Customer Solutions Engineer
- Extended Duo support access 18 hours per day (local time), 5 days a week to assist by a VIP support line
- Accountability for issue management and resolution

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Duo Security NEW

Expansion of Free Security Offerings
bit.ly/2UqY86W

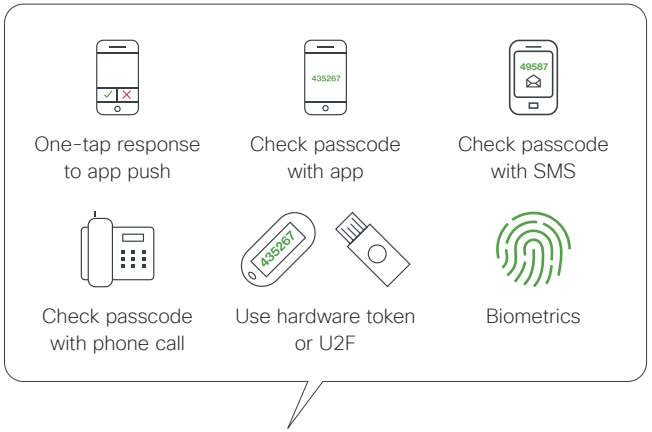
CISCO DESIGNED

Multi-Factor Authentication (MFA)

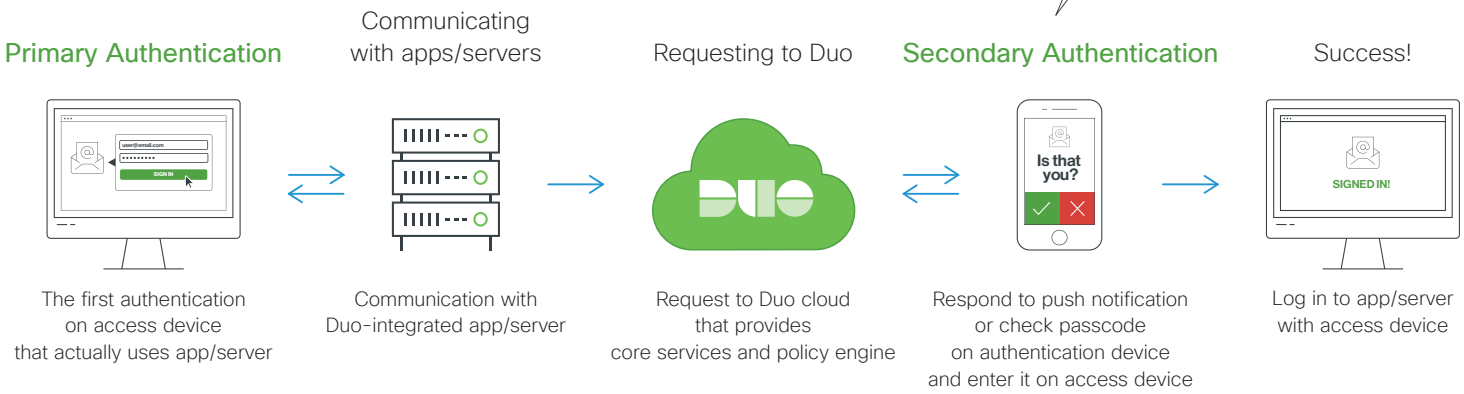
Multi-factor authentication from Duo protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. Duo is engineered to provide a simple, streamlined login experience for every user and application, and as a cloud-based solution, it integrates easily with your existing technology.
Adding multi-factor authentication to your security stack doesn't have to be disruptive to your users. Duo is fast and easy for users to set up, and with several available authentication methods, they can choose the one that best fits their workflow. No headaches, no interruptions — it just works.

- Benefits of Duo's MFA:
  - Verify your users' identities and protect against credential theft 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, and 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

Users can select various authentication methods by themselves



How it Works:



© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Duo Security NEW

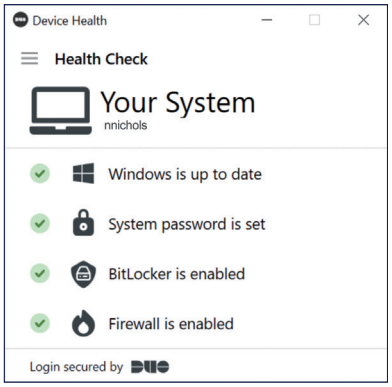
Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED

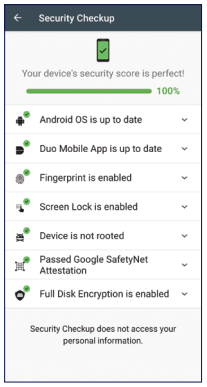
Device Trust

Secure access to the applications your users need, on the devices they want to use, from anywhere in the world. Gaining visibility into devices is the first step in establishing device trust, and it's an essential aspect of a strong zero-trust strategy. Duo provides visibility into every single device on your network and enforces health checks at every single login attempt. With Duo's Device Health, Security Checkup, and Self-Remediation features, users can take responsibility for the health of their laptops and mobile devices without help from IT. Automatically send reminders when it's time for a software update, and block out-of-date devices from accessing company resources.

- Benefits of Device Trust:
  - Visibility to inform security policies
  - Prevent compromised devices from introducing risk
  - Integrate with existing EMM/MDM solutions
  - Protect BYOD with lightweight solutions
  - 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



Duo Device Health Application for Desktop

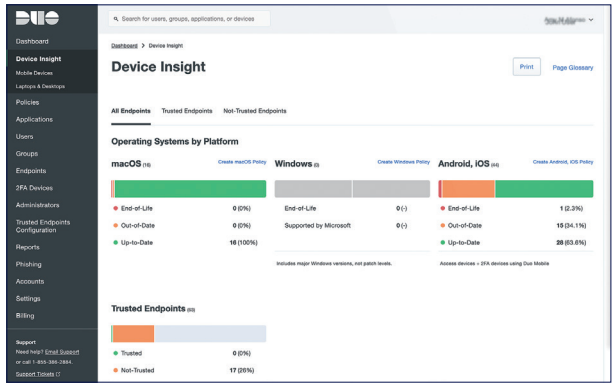


Security Checkup on Duo Mobile

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

Device Insight Dashboard

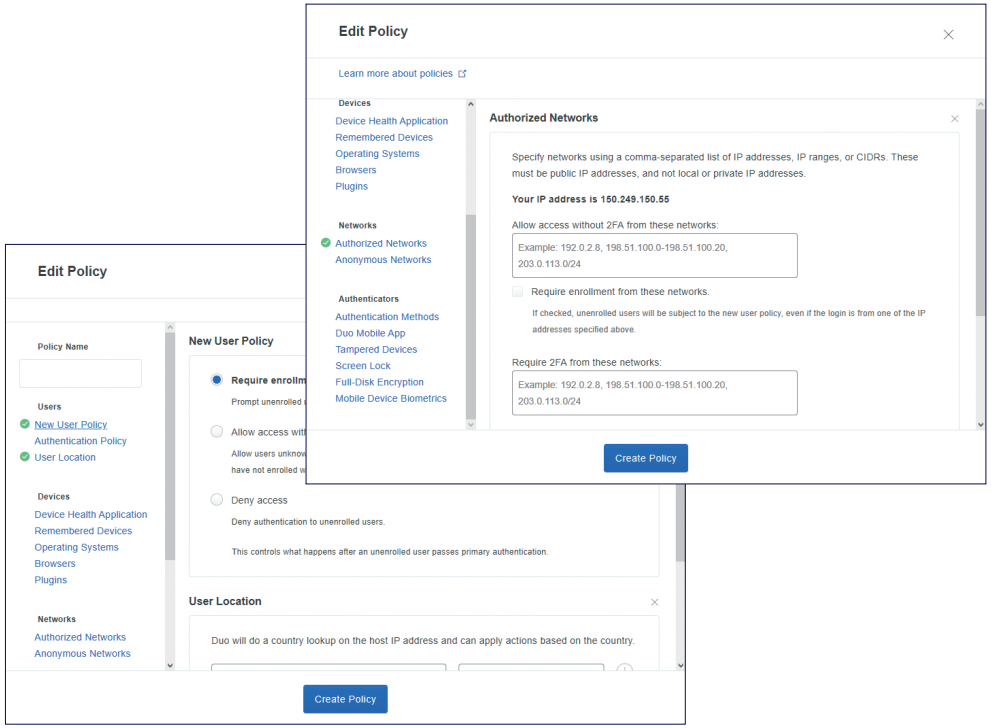


If any security risk exists on access device or authentication device, users can receive notifications on each device.

© 2020 Cisco and/or its affiliates. All rights reserved.

Adaptive Access Policies

A true zero-trust strategy changes the level of access or trust based on contextual data about the user or device requesting access. It also limits access to only users that really need it. With Duo, you can set up detailed policies in minutes via a simple, intuitive administrator dashboard, and manage rules globally or for specific applications or user groups.
Every user has a different use case for access to your applications, and Duo handles them all with ease. Detect key user information — like location, device, role, and more — at every login, and set security parameters that adapt to your users' ever-changing circumstances, without interrupting their workflow.



How adaptive authentication works:

- Enforce role-based access policies
  - Customize policies based on the user or group or their specific roles and responsibilities
  - Set custom policies based on authentication method
  - Only allow users to authenticate using certain methods (i.e., allow Duo Push, deny SMS)
  - Easily use Active Directory or Azure-AD user groups to apply policy
- 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
- Enforce app-specific policies
  - Enforce the use of more secure MFA methods (Duo Push, U2F, etc.) for high-risk applications and services
  - Restrict access based on geolocation
  - Prevent unauthorized access from any geographic location
  - Restrict access to any geographic location or require 2FA for certain locations
- Grant or block access by network
  - Grant or deny access to your applications based on where the user/device is coming from (set of IP ranges)
  - Block authentication attempts from anonymous networks like Tor, proxies, and VPNs

© 2020 Cisco and/or its affiliates. All rights reserved.

Remote Access

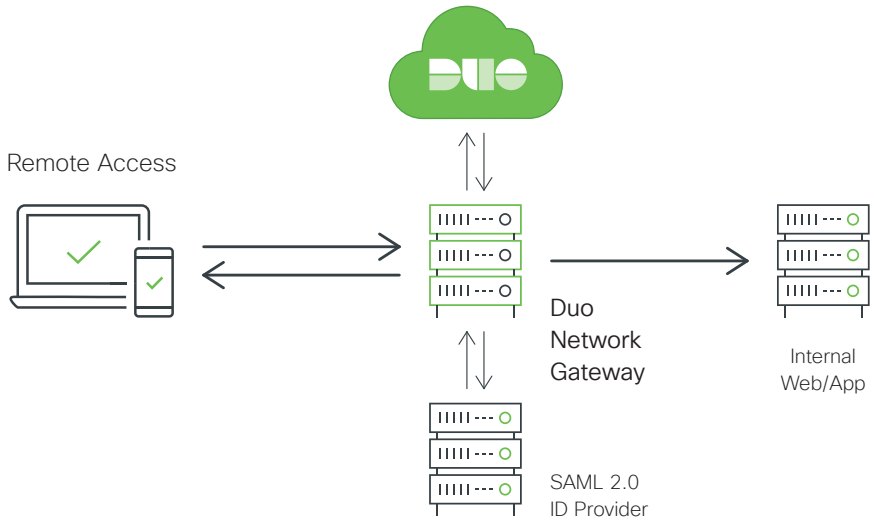
Enable an increasingly remote workforce with confidence. Duo's security solutions complement any technical environment, and they're engineered to verify identity and establish device trust no matter how, where, or when your users choose to log in.

Everyone's IT stack is unique, and Duo protects them all. Easily secure both on-premises and cloud environments — like Microsoft Azure, Amazon Web Services, and Google Cloud Platform — with or without a Virtual Private Network (VPN).

Duo's solution integrates seamlessly with major remote access gateway and VPN providers, including CA SiteMinder, Oracle Access Manager, Juniper, Cisco, Palo Alto Networks, F5, Citrix, and more.

Organizations can use Duo to apply the zero-trust principle of least privilege by allowing access to the applications they need using our policy control and securing applications behind the Duo Network Gateway.

With Duo Network Gateway, users can securely access internal web applications from any device, using any browser, from anywhere in the world, without having to install or configure remote access software on their device. Users can also remotely SSH to configured hosts through Duo Network Gateway after installing Duo's connectivity tool, providing perimeter-less access as an alternative to a VPN. Creating dedicated tunnels to critical applications and mitigating the potential for lateral movement by bad actors, in the event of a breach.



© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Duo Security NEW

Expansion of Free Security Offerings
bit.ly/2UqY86W

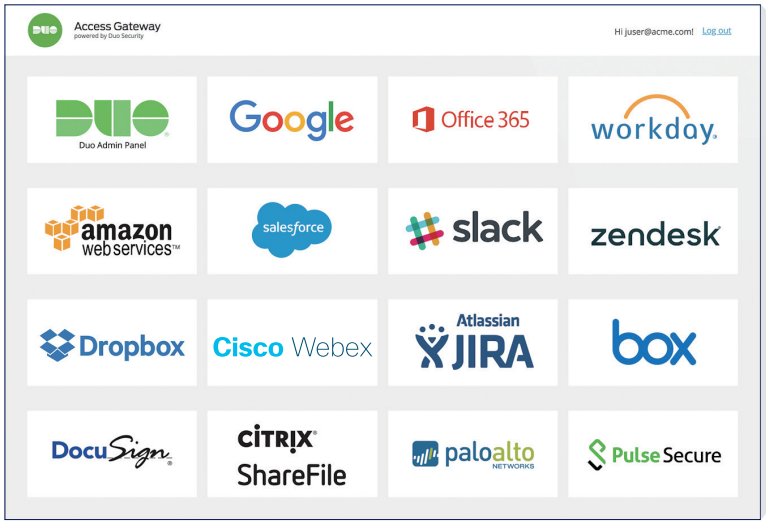
CISCO DESIGNED

Single Sign-On (SSO)

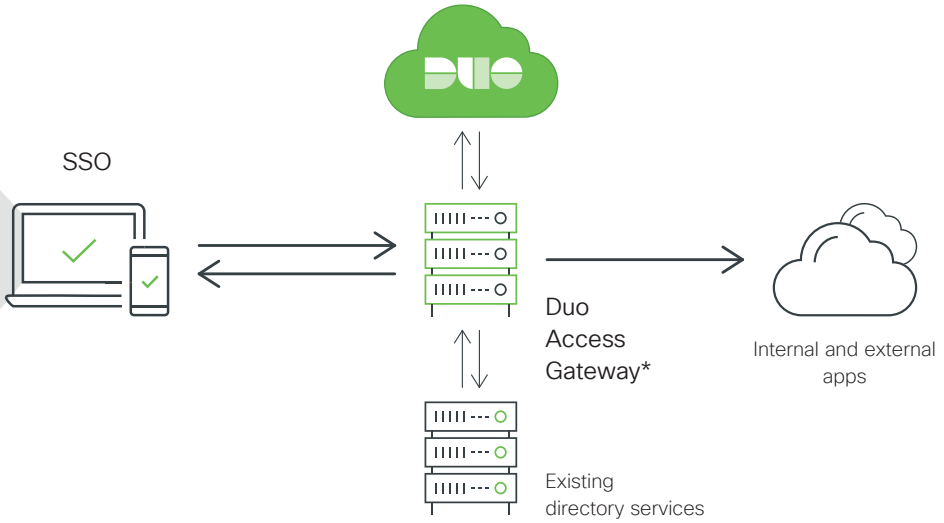
Today's workforce relies on an incredible variety of programs and platforms for productivity, and it can be difficult to provide on-demand access to these tools without compromising on security. Luckily, Duo safely puts essential applications at your users' fingertips. Whether you're looking for a new SSO solution or want to protect an existing one, Duo enables a streamlined login experience that's backed by airtight information security.

Duo's SSO is designed from a security-first perspective and allows you to configure access policies that can differ by application, depending on the sensitivity of its data, the privileges of the user and the device being used. This approach allows you to reduce user friction while protecting your most important assets.

With Duo Access Gateway, users can log in to a single, MFA-protected dashboard to gain access to all of their applications, both cloud-based and native. It's a true single sign-on experience.



Duo's SSO portal available to users



* Cloud version will be available soon.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Duo Security NEW

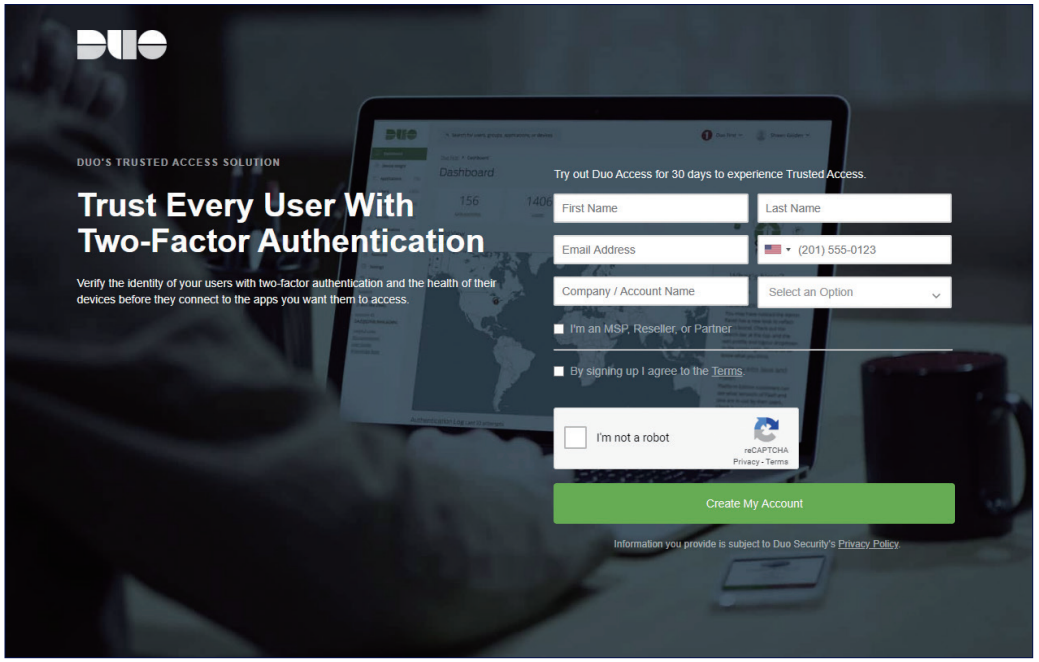
Expansion of Free Security Offerings
bit.ly/2UqY86W

CISCO DESIGNED

Free Duo Access 30-Day Trial

Sign up for a free 30-day trial and start securing your users in minutes with all of Duo's security features.

signup.duo.com/trial



Expansion of Free Security Offerings

With this offer, existing customers can exceed their user limit to support an increase in remote workers, and new customers can access a free license.

bit.ly/2UqY86W

	Existing Customers
Offer Details	Can exceed purchased user limit until end of offer period (1 July 2020)
Offer Period	Through 1 July 2020
Country/Region Availability	All regions where Umbrella is available for sale today.
Seller Action	No action is required for the seller. Email can be sent to customers impacted by COVID-19 and require support from Cisco.
Post-Offer Sales Engagement	At the end of the offer period, customers will either purchase the additional user licenses or reduce their usage to purchased user limits.
Technical On-boarding	None, customers are already deployed. The configuration of additional users is an existing process for the customer.
Support Details	Customers will be entitled to the same technical support they have purchased.

© 2020 Cisco and/or its affiliates. All rights reserved.