Zero Trust: Workforce

Solution Design Guide

Jan, 2020
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution overview</td>
<td>3</td>
</tr>
<tr>
<td>Getting started</td>
<td>6</td>
</tr>
<tr>
<td>Duo for workforce zero trust</td>
<td>12</td>
</tr>
<tr>
<td>Extend workforce trust</td>
<td>20</td>
</tr>
<tr>
<td>Ordering information</td>
<td>24</td>
</tr>
</tbody>
</table>
Solution overview

Today, the rise in a cloud-connected, mobile, and remote workforce has moved the visibility and control of users and devices outside of the enterprise. The perimeter has expanded beyond enterprise walls, making it more difficult for security and IT teams to verify user identities, and the trustworthiness of their devices, before granting both access to enterprise applications and data.

The new workforce model today requires an equally extended security model. The extended perimeter is now centered around user identity and their devices. The extended workforce security model must be able to establish device and user trust, no matter where the user is physically, and no matter what kind of network they’re connecting from.

Zero trust treats every access attempt as if it originates from an untrusted network. This model is focused on authenticating every user and device before granting access to any application. A zero-trust approach doesn’t require a complete reinvention of your infrastructure. The most successful solutions should layer on top of, and support, a hybrid environment without entirely replacing existing investments.

Ideal end state: Zero trust for the workforce

The ideal end state of your zero trust for the workforce solution would allow your enterprise to answer the following:

- **Are my users really who they say they are?** Verify the identity of every user, regardless of type (contractors, vendors, third-party providers, partners, remote users, employees, temporary workers, etc.).

- **What devices are connecting to my applications and data?** Get visibility into every type of device, both managed or unmanaged (mobile, laptops, and desktops; company-issued, -owned, or -managed; user-owned).
  - Visibility into the security health of these devices
  - Visibility into the security status of these devices

- **Who or what is allowed to access my applications and data?** By enforcing adaptive access policies, you can limit access to enterprise applications and data based on user role, type of device, security health of user devices, user group, application type, and much more.

- **How can I enable remote, frictionless access for all users?** With a remote-access proxy, you can enable access to multcloud environments, web applications, servers, VPNs, and more for employees, remote workers, and contractors. With Single Sign-On (SSO), you can allow users to securely access their cloud and on-premises applications seamlessly by logging in just once.
Cisco Zero Trust

A comprehensive approach to zero-trust security covers three key fronts of your IT ecosystem:

- **Workforce** – Ensure only the right users and secure devices can access applications.
- **Workloads** – Secure all connections within your apps, across a multicloud environment.
- **Workplace** – Secure all user and device connections across your environment, including Internet of Things (IoT).

Cisco Zero Trust provides a comprehensive approach to securing all access across your applications and environment, from any user, device, and location. It protects your workforce, workloads, and workplace.

Cisco Zero Trust methodology

Cisco takes a three-step methodology approach to implementing zero trust across your workforce, workloads, and workplace:

1. **Establish trust** – We verify the identity of users before granting access; check their devices for security posture and vulnerabilities; discover workloads; verify the trust of applications and services; and detect any indicators of a compromise.

2. **Enforce trust-based access** – With access policies and controls, we enforce least privilege access to applications, network resources, and workload communications and for all users and administrators of workloads.

3. **Continuously verify trust** – Finally, we verify that the original tenants used to establish trust are still true, and continually monitor traffic to ensure it’s not threat traffic. We also monitor for any risky, anomalous, and malicious behavior, and if compromised, then we change trust levels accordingly (by restricting or limiting access, isolating endpoints or servers, etc.).

This complete zero-trust security model allows you to mitigate, detect, and respond to risks across your environment. Verifying trust before granting access across your applications, devices, and networks can help protect against identity-based and other access security risks.

In this guide, we’ll only cover zero trust for the **workforce**.

Zero Trust for workforce

The scope of this guide will focus on zero trust as it relates to securing your workforce – that is, users and the devices they use to access work applications. Users may include employees, partners, vendors, contractors, and many others, making it more difficult to maintain control over their devices and access.

A zero-trust approach for the workforce should provide your organization the tools to be able to evaluate and make access decisions based on specific risk-based context as defined by your organization.

*For example* - Is the user verified using Multifactor Authentication (MFA)? Are their devices trusted and/or managed? Do their devices meet your security requirements?

Security teams need to be able to answer these questions to establish trust in users and devices accessing an organization’s assets. They also need to do it using an approach that balances security with usability.

This trust-centric security approach for the extended perimeter makes it much more difficult for attackers or unauthorized users to gain access to applications without meeting certain identity, device, and application-based criteria as defined by your organization.
Consider the following steps to take on your zero-trust journey toward securing your workforce:

1. **Establish user trust** - Can you verify that your users are who they say they are? Are you using a scalable, frictionless MFA solution? Using MFA and establishing user trust is the first step toward building a zero-trust model and protecting against compromised credentials, phishing, and other password-based attacks.

2. **Establish device trust** - Do you have visibility into every type of device accessing your applications? Can you check their security posture? And can you securely support all devices – BYOD (bring your own device), corporate-owned, and user-owned devices? At the time of login, check the trustworthiness of user devices to determine their security posture, no matter who manages or has control over the device.

3. **Enforce adaptive policies** - Can you enforce contextual policies based on user, device, and location to protect access to specific applications? By enforcing policies that evaluate risk based on attributes like location, user role, and device type, you can have more dynamic control over who and what can access certain applications – allowing only the minimum amount of access required for a user to do their job.

4. **Enable secure access to all applications** - Can you give your users a secure and consistent login experience to both on-premises and cloud applications? Implement MFA and device insight to enable secure access to all different types of applications, services, and platforms. The combination of both a trusted user and a trusted device makes it more difficult for an unauthorized user to pose as a legitimate one logging into your applications.

This guide will dive into each step and help you shape your criteria and requirements for the technology and solutions to provide secure trusted access from your users and their devices to work applications.

**Workforce threats**

With a zero-trust approach to securing the workforce, you can help prevent or mitigate against several different types of attacks that target users and devices in this new perimeter-less world:

**Identity-based attacks**

Attackers can easily steal or compromise passwords via phishing emails sent to users. With stolen credentials, they can log in to work applications or systems undetected and access data. Brute-force attacks involve programmatically trying different credential pairs until they work, another attack that can be launched remotely.

Once inside, attackers can move laterally to get access to more sensitive applications and data.

With multifactor authentication and device checks, you can establish trust in both a user’s identity and their device being used to access applications, preventing attackers that try to log in using only a password.
Device-based attacks

Devices running older versions of software – such as operating systems, browsers, plugins, etc. – can be susceptible to vulnerabilities not patched by software vendors. Without those security patches, devices that access work applications and data can introduce risks by increasing the overall attack surface.

Devices that don’t have certain security features enabled – such as encryption, firewalls, passwords, etc. – are also considered riskier or potentially out of compliance with data regulation standards that require encryption, like healthcare industry compliance standards.

Often, devices that are not owned or managed by your IT team can have out-of-date software and lax security.

With device trust features, you can establish trust in the device being used to access applications, preventing the potential spread of malware and introduction of vulnerabilities to your applications.

Getting started

The end goal is to remove the inherent trust model, and then replace it with a zero-trust approach that first establishes and verifies trust for all users and devices, before granting them access to applications and data.

Establish user trust

The first step toward architecting zero trust for your workforce is verifying your users’ identities when they log in to your cloud and on-premises work applications, services, and platforms.

Can you trust that your users are who they say they are? And how do you reduce the threat of compromised user credentials caused by phishing and compromised devices caused by malware and other vectors – while also meeting data regulatory compliance requirements for access security?

Multifactor authentication

Verify your users’ identities with a scalable, frictionless multifactor authentication (MFA) solution. This adds a second layer of trust that your users are who they say they are. After completing primary authentication (usually by entering a username and password), users verify their identity a second time, through a different channel (explained below). This reduces the likelihood that someone else can log in, since they would need both the password and their second factor to pose as the original user.

Support every user

Does your MFA solution provide flexible authentication options to fit a broad range of users, security profiles, and technical backgrounds? Make sure your solution supports employees, frequent travelers, contractors, vendors, customers, and partners.

You should be able to customize and enforce which MFA methods can be used. For more secure access to high-risk applications, require the use of:

- Easy-to-use, out-of-band mobile push notifications
- Phishing-proof Universal 2nd Factor (U2F) security keys
- Biometric-based WebAuthn
Other MFA methods support diverse user login scenarios:

- Phone callback for users who can't receive texts
- Mobile one-time passcodes for travelers while offline
- Text message passcodes for users without Internet connectivity
- Temporary bypass codes for contractors

Ease of administration

Is your MFA solution easy for administrators to deploy? Choose a cloud-based solution that requires minimal infrastructure and staff to roll out in order to reduce the burden on your team.

Does it provide user enrollment and provisioning options to scale as your organization grows? For example:

- Auto-enrollment
- Administrative APIs for scalable user provisioning
- Option to synchronize users from existing directories, such as Active Directory and Azure AD

Save on training, support, and ongoing help desk tickets with user self-enrollment and self-service - let your users enroll in MFA and manage their own authentication devices without administrative assistance.

Gain visibility into devices

Next, evaluate if your solution can give you insight into the devices connecting to your applications and data that you can leverage to control access based on device security health.

Do you have visibility across every type of end-user device - mobile, desktop, and laptops? Is there one tool that centralizes authentication and endpoint data across different device platforms? Can you easily get an overview of your users, endpoints, and authentication activity?

Device visibility

Get detailed insight into the security hygiene of every type of device (whether corporate managed or personally owned) accessing your applications.

Across every platform

Some device visibility solutions only give you limited insight into certain platforms and operating systems, like only those running Windows or desktops. Reduce the need to access different data systems with one centralized dashboard that gives admins oversight across:

- All desktops, laptops, and mobile devices, whether corporate or personally owned
- Operating systems: Windows, Mac, iOS, Android, etc. (versions, number of out-of-date devices)
- Browsers: Chrome, Firefox, Edge, Internet Explorer, etc. (versions, number of out-of-date devices)
- Plug-ins: Java and Flash (versions, number of out-of-date devices, enabled, disabled, or uninstalled)
Support BYOD and Mobile

The extended perimeter presents new challenges around securing BYOD (bring your own device). A zero-trust model should both work well with your existing infrastructure without causing friction, and support any type of device.

You should be able to get insight into personal and corporate-owned devices, including mobile devices. BYO devices may not meet security requirements or may be running older software versions prone to vulnerabilities.

A comprehensive device visibility solution should let you identify mobile devices with certain security features enabled or disabled, as well as their security posture:

- iOS or Android version
- Disk encryption
- Jailbroken, rooted, or tampered with
- Biometrics (fingerprint, touch, or face ID)
- Screen lock

Device logs and reports

Many compliance regulations and auditors require user activity and device security logs and reports. Can your device visibility solution give you access to detailed reports on user behavior and risky devices - all in one dashboard? Does it integrate nicely with any existing SIEM (security information and event management) software?

Make sure your admins have easily accessible and exportable reports for auditors, with insight into authentications, users, admins, policies, and more.

Establish device trust

At login, check the security health of all user devices attempting to access your applications. Establishing trust extends beyond managing the status of the device to include inspecting and controlling access based on mobile and personally owned devices.

Can you enforce endpoint controls for risky devices or corporate-owned devices? How are you establishing mobile device trust? Are you able to automatically notify users of out-of-date software to reduce your help desk tickets?

Enforce endpoint controls

By leveraging the visibility of devices connecting to your applications (as discussed previously), you should be able to establish device-based access policies to prevent any risky or untrusted devices from accessing your applications.
**Risk-based device access**

For access to high-risk applications, you may require a device to be corporate-owned or managed by your organization’s IT team. Example of high-risk applications may include Electronic Health Record (EHR) systems like Epic that contain patient health information, cloud infrastructure like Microsoft Azure and Google Cloud Platform, and many others.

Can you enforce access policies based on the application risk or whether the device is corporate or personally owned? And can you do this without requiring endpoint certificates?

Additionally, you may require MFA for access to more sensitive applications for a higher level of assurance of your users’ identities. Can you require your users to use push notifications, U2F security keys, or biometric-based WebAuthn before granting them access to certain applications?

**Establish mobile device trust**

Make sure your solution allows you to establish mobile device trust with or without the use of Mobile Device Management (MDM) software.

Users may object to installing MDMs on their personal devices due to privacy concerns, resulting in lower overall adoption and reduced insight into their device security. And sometimes it’s outside of your IT team’s control to install an agent on the personal devices of third-party providers that may need access to your applications.

Whether or not you have an MDM solution, you should be able to block devices from accessing your applications based on:

- OS, browser, and plug-in versions and how long they’ve been out of date
- Status of enabled security features (configured or disabled)
- Full disk encryption
- Mobile device biometrics (face ID/touch ID)
- Screen lock
- Tampered (jailbroken, rooted, or failed Google’s SafetyNet)

**Notify users to update risky devices**

Does your solution enable your users to manage their own devices? Choose a solution that can detect older software versions, and then notify users when their device software is out of date.

To relieve the burden on your help desk support team, prompt users to update the software on their own devices at login. A self-service portal also allows them to easily manage their own authentication devices without submitting a help desk ticket.
Enforce adaptive policies

Enforce contextual access policies allowing access to your applications with user-, device-, and location-based controls. The context includes different aspects of their login attempt - where they’re located, what role they have in your organization, what type of device they’re using, etc.

Limit access to only what your users need to do their jobs and add stricter controls for access to more sensitive applications - without negatively impacting user workflows. Can you customize policies based on users, user groups, or user location? Or challenge users with a more secure MFA method, based on what application they’re accessing?

Contextual access policies

Customize policies to allow, deny, or require stricter security based on user-specific roles and responsibilities, devices, and applications - all while balancing security with usability.

Role-based access policies

Not all users need access to every application - can you customize access based on the type of user group? Give contractors or third-party providers temporary and restricted access to nonsensitive applications or systems.

You should be able to enforce policies to grant a higher level of access to admins and privileged users, while ensuring only developers have access to your production environments and cloud infrastructure.

Check that your admins can:

- Customize policies based on the user, group, or their specific roles and responsibilities
- Set custom policies based on authentication method
- Only allow users to authenticate using certain methods
- Easily use Active Directory or Azure AD user groups to apply policy

App-specific policies

Enforce the use of more secure MFA methods for access to business-critical applications and services to reduce the risk of unauthorized access.

Your admins should be able to configure app-specific policies to require only the use of push-based or U2F security keys to verify your users’ identities before granting access to these applications. The required use of only more secure methods provides a higher level of assurance of user identity, strengthening access control to your more sensitive applications and data.

User location

Prevent unauthorized access from any geographic location with user-based access policies. If you don’t do business in certain countries, you should be able to block access attempts originating from those regions.

Admins should also be able to block authentication attempts based on a set of IP address ranges or those coming from anonymous networks like Tor or proxies. However, nonblocked IP addresses do not imply that access is allowed – this is only one attribute to consider in the broader context of an access request.
Enable secure access to all applications

Give users secure and consistent access to all applications, services, and platforms, no matter where they are hosted.

Protect your investments

You may be a cloud-forward organization, or a large enterprise with a complex mix of both cloud and legacy on-premises infrastructure and applications. Whatever it is, make sure you can protect access to all of it with MFA, contextual access policies, and device visibility and controls.

Remote access

The shift to cloud infrastructure has made it challenging for organizations to apply stronger access controls across hybrid and multicloud environments.

Your solution should simplify and keep the user login experience consistent, no matter where users are located, when they’re connecting to various systems and applications hosted in different cloud environments.

Make sure you can secure access to:

- Multicloud environments, such as Azure, AWS, and Google Cloud Platform
- Infrastructure, dev/DevOps environments, and internal Linux servers
- HTTPS web applications and SSH servers
- Virtual Private Network (VPN) and remote access applications

Enforce stronger security controls to only allow managed, up-to-date devices access to infrastructure and developer environments.

Cloud/identity access

Secure access to all of your cloud apps such as Office 365, Google, Box, Dropbox, Slack, and more, as well as access to any existing Single Sign-On (SSO), identity providers, and federation services. Make sure your solution provides secure access to any SAML 2.0-enabled cloud application.

Best practices recommend securing access to these apps by separating your primary authentication method from your secondary (using MFA). Shift away from depending solely on a primary authentication provider to avoid a vendor-based breach that can risk exposing both primary and secondary authentication.

Secure Single Sign-On (SSO)

For a consistent login experience, let your users log in once to access all of their cloud and internal work applications with a secure Single Sign-On (SSO) solution.

Protect your SSO with MFA and contextual access policies and check the security of your users’ devices each time before granting access.
Duo for workforce zero trust

This guide will walk you through the key stages when designing and rolling out your zero-trust solution using Duo, along with the best practices and key resources for each step of the way. The aim is to make your deployment as easy and as successful as possible.

Success planning is where you will begin designing your Duo deployment. We have developed a deployment timeline (see below) based on successful Duo deployments. This can serve as a blueprint for your Duo rollout. Each key Duo deployment stage is emphasized in black, accompanied by key tasks to be completed during the stage.

**Administration overview**

You will need to assign Duo administrators various roles to manage users, policy settings, applications, and more. Configuring alerts and messaging will also help prevent snags in the deployment process.

**Best practices**

- Only Duo administrators with the “Owner” role can create, update, or delete other Duo admins. Because of this, we recommend having at least two administrators with the Owner role within the account.
- Specify a [Lockout and Fraud Reporting](#) email address. We recommend a distribution list so that multiple people have visibility to those alerts.
- Customize the help message shown to your users in the Duo browser prompt with the [Help Desk Message Setting](#).
- If your organization consumes a large volume of telephony credits, set up the [Low Telephony Credit Alert option](#).
Consider leveraging Administrative Units to control how administrators can view and manage groups of Duo users and applications.

If you have an SAML 2.0 identity provider, you may configure single sign-on (SSO) login to the Duo Admin Panel.

Key resources

- Admin Panel Settings Overview
- Managing Duo Administrators
- Duo Administrative Roles
- Help Desk Guide
- Telephony Credits: Low Credit Alert
- How-to: Custom Duo Prompt Help Messaging
- Lockout and Fraud Reporting
- Duo Liftoff Guide

Establishing user trust with Duo

Determine Duo enrollment methods

Best practices

- Duo recommends syncing users from an external directory to reduce the administrative burden for provisioning and deprovisioning users.
• Customize the email sent to your synchronized users by enabling the Send Enrollment Email to Synced Users option. You can choose to include your company logo in the enrollment email.

• Understand the difference between Duo user enrollment states.

Key resources

• User Enrollment Options

• The Duo Policy Guide includes information on how policy configuration can affect user enrollment

Identify applications

Duo can protect a wide variety of on-premises and cloud-based applications through both preconfigured solutions and generic configurations via SAML, RADIUS, LDAP, and more.

Best practices

• Read over the Duo documentation for applications you have in mind and note any prerequisites, such as the Authentication Proxy, Duo Access Gateway, or an SAML Identity Provider that could take additional time or resources to prepare.

• Widely used and highly sensitive applications are great starting points:
  ◦ Applications that cover a majority of users will help tie enrollment and go-live together. Office 365 is a great example of this – many people use email, calendaring, and other productivity tools. This way, most of your users are enrolled and familiarized with the 2FA experience early on.
  ◦ You can immediately prioritize the security of your systems and applications that contain or have direct access to sensitive data by making them part of your initial Duo rollout.

Considerations

• Is there a compliance need? Is there a deadline set by PCI, HIPAA, DEA, or internally by a CISO or other lead?

• What are your resources for deployment? Are test environments available? If your organization has a small IT staff or staff with limited technical bandwidth, you may want to choose a native or less-complex application integration and then iterate to expand the scope of your Duo project in phases. If you have many resources, you might consider deploying multiple applications at the same time.

• What will the user experience be like for the application you choose? Consider your users’ willingness to adopt 2FA. Select applications that present the Duo Prompt for enrollment and self-service, or choose to first enroll user groups that will be quick to adopt 2FA.

• Was there a security incident involving a specific application or user population that is a high-value target?

• Is there a certain time of year that puts a strain on your organization or IT staff (for example, the start of the school year for educational institutions, or November and December for retail organizations)? If you’re a tax firm, March and April may not be the best time to institute a new IT project.
• Once you have your most largely used and at-risk applications protected, you might next consider protecting:
  ◦ HR portals or payroll systems
  ◦ Privileged access
  ◦ Remote access
  ◦ Standalone web applications or cloud identity management solutions

Key resources

• List of supported applications and features by edition

• Many of Duo’s application integrations do not require any local components. However, certain functions do require a local Authentication Proxy service. The Authentication Proxy Reference Guide contains a comprehensive reference of configuration options available for the proxy. Generic RADIUS and LDAP documentation is available as well.

• The Duo Access Gateway, Duo’s SSO solution, protects access to cloud-based applications and creates a web-based application launcher page for your organization: https://duo.com/product/every-application/single-sign-on.

• The Duo Network Gateway provides remote access to on-premises applications with multifactor authentication and device inspection using the Duo Prompt. It can be connected to the Duo Access Gateway or any SAML IdP. Links to on-premises web applications can be added to the application launcher to make them easy for employees to locate.
Configure applications with Duo

**Best practices**

- Duo can be installed and configured to protect many of our supported applications in a variety of ways. This allows you to build your Duo applications to give you the end-user and administrative experiences you desire.
  - You can find more details in our [Application Documentation](#) and [Knowledge Base](#).
- Give your applications meaningful names in the Duo Admin Panel.
  - The application name is displayed prominently in Duo push requests to end users. This helps users identify which application is initiating the 2FA request.
  - Descriptive application names make it easier to find applications in the Duo Admin Panel and filter the authentication log results.
- Treat your application SKEY like you would a privileged password. Do not ever send the SKEY as a screenshot or plaintext over email, even to Duo support technicians! If you do need to transmit your SKEY, we recommend a SHA-256 hash.

**Key resources**

- [How-to: Protecting Applications](#)
- [Application Configuration Documentation](#)
- [How-to Videos: Application Integrations](#)
- [Authentication Proxy Reference Guide](#)
- [Authentication Proxy Best Practice Guide](#)
Test your Duo applications

Best practices

- Test your Duo applications in a nonproduction environment. This allows you to identify potential issues before your end users encounter them.
  - There is no limit to the number of Duo applications you can set up. We recommend building a Duo integration in a lab environment or virtual machine before deploying to end users.
  - If you are using the Duo Network Gateway to provide SSH or application access to on-premises applications, we recommend conducting a test that ensures you are able to access those applications from outside your network without the use of your VPN client.
- Label your applications in the Duo Admin Panel accordingly to reflect their usage in your test or production environments.
  - Example: Eng-SSH-TEST and Eng-SSH-PROD are two separate Duo Unix applications configured the same for testing and production, respectively.

High availability and disaster recovery configuration

Best practices

- Understand the Duo failmode options and which integrations support them.
  - Authentication workflows that involve the Duo Authentication Proxy, as well as most installer-based integrations like Winlogon/RDP and UNIX PAM, generally allow you to configure a failmode.
- Have an emergency plan for how to remove Duo from the authentication workflow in the event of a long service disruption.
  - This should be done on a per-application basis.

Key resources

- Duo Guide to Business Continuity Preparedness
- Setting up the Duo Authentication Proxy for High Availability and Disaster Recovery
- Setting up the Duo Access Gateway for High Availability
- Setting up the Duo Network Gateway for High Availability

Conduct an end-user pilot

Best practices

- We recommend piloting Duo in multiple phases to ensure a successful and smooth deployment.
  - PHASE 1: Test with a pilot group of IT or technical users to ensure that the technology works and the login experience matches what you’re looking for.
  - PHASE 2: Once you have worked out the login experience with your IT group, deploy to a small subset of nontechnical business users to determine user education gaps and what to expect when deploying at scale.
Key resources

- Deploying a Proof of Concept

Establishing device trust with Duo

Configure and Test Trusted Endpoints

Best practices

- The Trusted Endpoints Global Policy defaults to checking devices for trust but never blocks access if the device is untrusted. We recommend leaving the default global setting and configuring additional policies applied to applications or user groups to allow or disallow based on their trust status.

- Consider using the Trusted Endpoints with Duo Mobile integration to ensure that end users’ mobile devices are checked for security posture every time they are used to access a secured application. Note that once enabled, the user will be prompted to open Duo Mobile to perform a device health check prior to authentication.

Testing and Troubleshooting Trusted Endpoints

- Every organization is different, which can affect how you may want to roll out and enforce this feature. Common deployment scenarios are documented in our Deployment Setup Tips.

- We recommend testing to understand the end-user experience:
  - Will users encounter any additional prompts during authentication?
  - Are users blocked when attempting access from an untrusted device when a blocking policy is configured?

- As part of a comprehensive test plan, consider testing application access with:
  - Multiple OSes, including mobile OSes like Android and iOS
  - Thick applications on both desktops and mobile devices (if applicable)
  - A variety of browsers, including mobile browsers

- If using the Manual Enrollment integration for testing, note that downloading and installing a certificate for manual enrollment on the test device does not mean that the device will be checked for trust. Be sure to add the user associated with that test device to a test user group, then associate that test group with the Manual Enrollment integration. Also note that a Manual Enrollment certificate is only associated with the user who first uses it. However, multiple certificates for separate user logins on one machine are supported.

- Troubleshooting: Reference our Trusted Endpoints Knowledge Base articles for a list of common questions and issues related to Trusted Endpoints.

Key resources

- Trusted Endpoints documentation
- Trusted Endpoints Best Practices Guide
- How Duo establishes Device Trust
- Trusted Endpoints Knowledge Base articles
Enforce adaptive policies with Duo

Customize user access with Duo policies

Best practices

- Keep in mind that enrollment, group, and user statuses can impact policy implementations.
- Some policy implementation scenarios will require both an application and a group policy to achieve the desired outcomes.
- As a start, here are some of the most popular policy controls other Duo customers implement that you might consider for your rollout:
  - Require users to have the most up-to-date version of Duo Mobile
  - Require that mobile users enable screen lock
  - Require that users are on the latest version of iOS or have the latest security patches on Android
  - Require that users’ Windows and MacOS devices meet your organization’s security policy using the Device Health App
  - Allow access to users using only devices verified by the Device Health App
  - Allow access to users using only Trusted Endpoints
  - Deny access from anonymous IPs
  - Deny access from nonsupported browsers

Key resources

- Policy and control documentation
- Duo Policy Guide: Configuring Access via Duo’s Policy Engine
- Device Health Application documentation

Continuously verify trust with Duo

Continuously monitor risky devices

Best practices

- Use adaptive polices to verify device security health and status. If a device’s security health or status has changed, the device will not be allowed to access further applications
- Extend workforce trust by integrating Duo with Cisco® Advanced Malware Protection (AMP) for Endpoints. Once integrated, Duo and AMP for Endpoints work together to detect malware and automatically respond to threats by blocking risky endpoints with access policies.
Key resources

- Unified Endpoint Visibility (Device Insight) documentation
- Endpoints documentation
- Device Access Control documentation
- Trusted Endpoints documentation
- Device Health Application documentation

Extend workforce trust

Extend your protection of the workforce by tapping into additional integrated capabilities to better protect and detect threats.

Cisco AMP (Advanced Malware Protection) for Endpoints

Global Threat Intelligence

Cisco Talos® experts analyze millions of malware samples and terabytes of data per day and push that intelligence to AMP. AMP then correlates files, telemetry data, and file behavior against this context-rich knowledge base to proactively defend against known and emerging threats.

Advanced sandboxing

Advanced sandboxing capabilities perform automated static and dynamic analysis of files against more than 700 behavioral indicators. These analyses uncover stealthy threats and help your security team understand, prioritize, and block sophisticated attacks.

Point-in-time malware detection and blocking

Block malware trying to enter your network in real time. Using AV detection engines, one-to-one signature matching, machine learning, and fuzzy fingerprinting, AMP analyzes files at point of entry to catch known and unknown malware. The result? Faster time to detection and automatic protection.

Continuous analysis and retrospective security

Once a file enters your network, AMP continues to watch, analyze, and record its activity, regardless of the file’s disposition. If malicious behavior is spotted later, AMP sends your security team a retrospective alert that tells them where the malware came from, where it’s been, and what it’s doing. In a few clicks, you can contain and remediate it.
Establishing endpoint trust before a user logs in to an application with their device is a key aspect of overall workforce security. When paired with establishing user trust, the combination gives your enterprise stronger assurance of their identity and security posture.

**Duo Security** and **AMP (Advanced Malware Protection) for Endpoints**, once integrated, work together to detect malware and automatically respond to threats by blocking risky endpoints with access policies.

Duo evaluates the health of the device and security status on every access attempt, then blocks access from endpoints that don’t meet your security policies. Duo prompts users to remediate their own devices when access has been denied.

AMP for Endpoints uses global threat intelligence to automatically block known malware and also detects threats with continuous file monitoring. Then AMP for Endpoints rapidly contains attacks by isolating infected endpoints. Through the Duo and AMP for Endpoints API integration, application access will be blocked if the device has been compromised. Once the compromised device has been resolved within AMP for Endpoints, Duo resumes access to the application with its existing set of security controls.

**Key resources**

- [Cisco AMP for Endpoints](#)
- [Cisco AMP for Endpoints Data Sheet](#)
- [Cisco AMP for Endpoints Deployment Methodology and Best Practices](#)
- [Trusted Endpoints and AMP for Endpoints Integration](#)
- [Cisco Multicloud: Cloud Protect Design and Deployment Guide Including Cisco Umbrella and AMP for Endpoints](#)

**Umbrella**

Cisco Umbrella™ is a cloud security platform that provides the first line of defense against threats on the Internet wherever users go. And because it’s built into the foundation of the Internet and delivered from the cloud, Umbrella is the simplest security product to deploy and delivers powerful, effective protection. Umbrella combines multiple security capabilities into a single cloud security service.
DNS-layer security
Umbrella’s DNS-layer security provides the fastest, easiest way to improve your security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

Secure web gateway
Umbrella’s secure web gateway logs and inspects web traffic for full visibility, URL and application controls, and protection against malware. Use IPsec tunnels, PAC files, or proxy chaining to forward traffic to our cloud-based proxy to enforce acceptable use policies and block advanced threats.

Cloud-delivered firewall
Umbrella’s firewall logs all activity and blocks unwanted traffic using IP, port, and protocol rules. To forward traffic, simply configure an IPsec tunnel from any network device. As new tunnels are created, policies are automatically applied for easy setup and consistent enforcement everywhere.

Cloud access security broker
Umbrella exposes shadow IT by providing the ability to detect and report on cloud applications in use across your organization. For discovered apps, view details on vendor, category, and activity volume to better manage cloud adoption and reduce risk.
Interactive threat intelligence

Our unique view of the Internet gives us unprecedented insight into malicious domains, IPs, and URLs. Available via a console and API, Umbrella Investigate provides real-time context on malware, phishing, botnets, Trojans, and other threats, enabling faster incident investigation and response.

Integration with SD-WAN

The Umbrella and Cisco SD-WAN integration deploys easily across your network for powerful cloud security and protection against Internet threats. Our integrated approach secures cloud access and efficiently protects your branch users, connected devices, and app usage from all direct Internet access breakouts.

Key resources

- Cisco Umbrella
- Cisco Umbrella Data Sheets
- Cisco Umbrella Solution Sheets
- Cisco Umbrella Documentation
- Duo Protection for Umbrella

Use case: Secure Office 365

Securely use Office 365 and defend against phishing and advanced threats

Cisco provides an invisible layer of security that won’t disrupt user productivity. Cisco offers the ability to add additional layers of security to protect Office 365 and many other Microsoft applications.

Securely log in with Duo MFA

At the point of Office 365 application access, verify user identity and device trust with Duo.

- Verify users' identities with strong MFA for all applications.
- Enforce adaptive policies by establishing device trust, security posture, and location.
- Enforce compliance policies by verifying that devices are encrypted and password protected.
- Enforce role-based access control to applications with sensitive information.
Added protection against malicious Links with Umbrella

**Stop security threats from any source easily.**

- Block requests from any source (email, SMS, web, etc.) to phishing, malware, ransomware, and botnets before a connection is even established.
- Block access to specific cloud applications for data loss prevention (prevent users from copying data to cloud storage locations, personal email, etc.).

Establish device trust and protect against endpoint threats with AMP for Endpoints

**Protect endpoints** from malware, ransomware, and viruses, while blocking compromised devices from accessing applications.

- Protect the endpoint from malicious attachments and other applications that may end up on the device.
- Respond to threats by isolating the endpoint from networks when a compromise is detected.
- Through the integration of AMP for Endpoints with Duo, block the endpoint from accessing other applications until compromise has been resolved.

Ordering information

**Editions**

**Cisco Duo MFA**

Full-featured, two-factor authentication for every organization.

- Protect logins with Duo’s MFA (multifactor authentication)
- Insight into an overview of device security hygiene
- Manage Duo’s solution with Admin APIs
- Provide secure Single Sign-On (SSO), enabling a consistent user login workflow across all applications
- Protect access to both on-premises and cloud applications

**Cisco Duo Access**

Includes everything in Duo MFA, plus:

Essential access security suite to address cloud, BYOD, and mobile risks

- Complete visibility into both mobile, laptops, and desktops, including corporate-managed and unmanaged (personally owned) devices to support BYOD policies
  - Mobile device breakdown with visibility into enabled security features and tampered/unencrypted devices
- Assign and enforce security policies globally or per application (based on user’s location or network, or per user group)
- Notify users to update their devices based on device access policies
• Full-featured dashboards and custom reports for compliance audits and ease of administrative management

• Secure Single Sign-On (SSO) for all cloud applications

Cisco Duo Beyond

Includes everything in Duo Access, plus:

A zero-trust security platform that addresses user and device risk for every application

• Get visibility into BYOD – detect if devices (laptops, desktops, and mobile) are corporate-managed or unmanaged (personally owned)
  ◦ Identify if a third-party agent is enabled on the device (such as antivirus)

• Enforce a policy to allow only managed devices access to sensitive applications
  ◦ Limit mobile device access to applications based on enrollment in endpoint management systems or MDM enrollment

• Provide modern remote access to multicloud environments (on-premises, Azure, AWS, Google Cloud Platform) while enforcing zero-trust security principles

• Secure access for internal web applications and servers via SSH

<table>
<thead>
<tr>
<th></th>
<th>Duo MFA</th>
<th>Duo Access</th>
<th>Duo Beyond</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFA with Duo Push for iOS and Android</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MFA with security keys, U2F, OTP, phone callback, SMS, and hardware tokens</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Telephony credits</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>100 credits/user/year</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User self-enrollment and self-management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A dashboard of all devices accessing applications</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Monitor and identify risky devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Visibility into security health of laptops and desktops (Duo Device Health application)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Visibility into security health of mobile devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identify corporate-owned versus BYOD laptops and desktops</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Identify corporate-owned versus BYOD mobile devices</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Duo MFA</td>
<td>Duo Access</td>
<td>Duo Beyond</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Identify if a third-party agent is enabled on the device (for example, antivirus, antimalware)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Adaptive Auth and Policy Enforcement</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Assign and enforce security policies globally or per application</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enforce policies based on authorized networks</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforce policies based on user's location</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Assign and enforce security policies per user group</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Block Tor and anonymous networks</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Enforce device trust policies based on security health of laptops and desktops (out-of-date software, encryption, firewall, etc.)</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enforce device trust policies based on security health of mobile devices (encryption, tampered, screen lock, biometrics)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notify users to remediate their devices (self-remediation)</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Limit device access to applications based on enrollment in endpoint management systems such as LANDesk, JAMF, and Microsoft Intune</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Limit mobile access to applications based on enrollment in MDMs (AirWatch, MobileIron, Microsoft Intune)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Secure Application Access and Single Sign-On (SSO)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Unlimited application integrations</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SSO for all cloud applications</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Secure access to internal company web applications (Duo Network Gateway)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Secure access to specific internal servers via SSH (Duo Network Gateway)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Secure remote access to applications hosted in AWS, Azure, and GCP (Duo Network Gateway)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Duo on global price list

Duo is on the Global Price List. Please check orderability for your country on the Duo SalesConnect Page. Orders for Duo involve four SKU types:

- The subscription SKU is used to define the subscription term and start date.
- The product SKUs are used to define the products and quantities that make up the subscription.
- The product add-on SKU can only be added on to other product SKUs.
- The support SKU defines the level of support for the subscription.

Key resources

- Duo Ordering Guide