Duo Trusted Endpoints

Establish trust in managed and unmanaged devices

> “**Duo became the link we needed to make our security philosophy really work.** We now know that if folks were downloading reports or manipulating data in a cloud application, that they were doing it from a safe device, and that their identity had been confirmed with MFA.”

Simon Duffey, Senior IT Manager and Service Owner for Productivity and IT Security, Certinia

Benefits

- Distinguish between managed and unmanaged endpoints that access your browser-based applications
- Restrict access to only known and trusted devices enrolled in a device management solution or registered with Duo
- Build a customized inventory of trusted devices that includes managed devices and unmanaged registered endpoints
- Extend your security coverage to include Duo registered, unmanaged BYO (Bring Your Own) and third-party devices
- Verify endpoint trust to block attackers from accessing applications using unknown devices
- Meet data security regulations and privacy laws that require security controls to block risky devices and ensure only those that are secure have access
- Combine Cisco Secure Endpoint with Duo Trusted Endpoints to identify and block malware-infected endpoints

Duo Trusted Endpoints lets you define and manage trusted endpoints and grant secure access to your organization's applications with custom policies. The Trusted Endpoints policy verifies whether devices accessing the applications are company managed or registered with Duo, and blocks access from devices that aren't.

Block Attackers

Only allow registered or managed devices to gain access to corporate apps and resources

Control Device Access

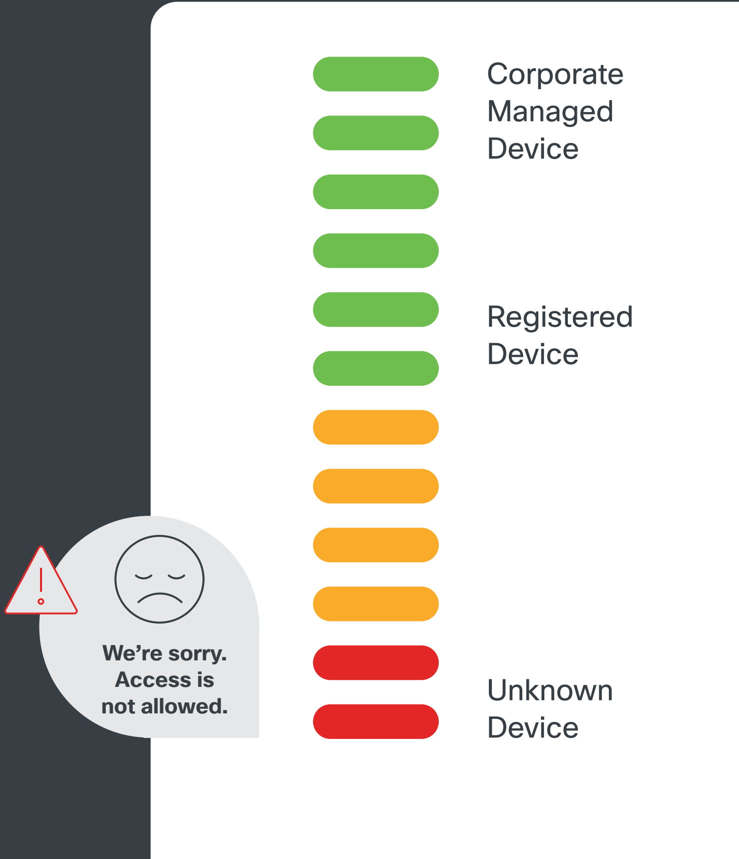
Give organizations control over which devices can access corporate apps and resources

Cover BYOD

Safely allow Bring Your Own Device (BYOD) and 3rd-party devices without requiring Mobile Device Management software

Mitigate Risk

When limited authenticator options are available



Addressing a New Reality with Trusted Endpoints

The way we approach work has changed significantly over the past few years. Our new reality includes a hybrid work environment with a blended workforce. To maintain productivity and steady workflows, organizations must enable secure and direct access to corporate applications and data for a diverse set of users (remote workers, contractors and partners) and their devices that typically reside outside of the control of corporate EMM (enterprise mobility management) and MDM (mobile device management) solutions.

Enforcing consistent access security policies across company-issued and managed devices, BYOD and third-party (contractor or partner) devices to establish trustworthiness poses significant challenges. You could require every endpoint to be managed, however owners of personal devices are often reluctant to install management software that gives the organization control over their endpoint. You could also extend trust to unmanaged personal devices as well as those used by your partners.

However, allowing access from unknown and untrusted devices introduces risk. And when you allow direct access to cloud applications over the internet, the devices don’t touch your network so traditional network access controls can’t be applied. Adding to the complexity, IT security teams often lack the necessary insights and enforcement mechanisms when making an access decision on endpoints, particularly among unmanaged devices.

Enable Secure Application Access with Trusted Endpoints

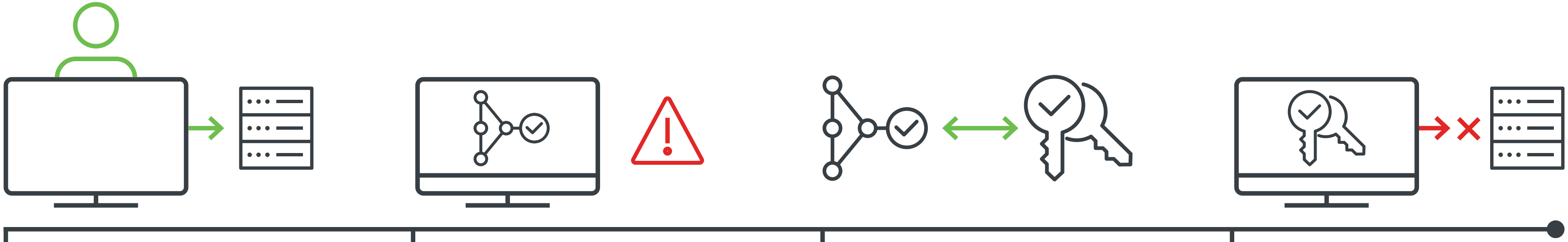
Available in every Duo paid edition, Duo Trusted Endpoints provides the controls to block unauthorized access by allowing only managed or registered devices to gain access to corporate resources. Create and enforce a custom Trusted Endpoints policy that grants application access to corporate-issued and managed devices and decide whether to extend trust to unmanaged personal devices as part of your BYOD strategy. When allowing direct access to cloud-hosted applications, Duo serves as the enforcement point each time a user authenticates so your access control policies are applied. Duo supports integrations with a broad range of leading enterprise device management solutions so you can use your favorite third-party solutions. You can add an additional layer of protection by combining your Trusted Endpoints policy with Cisco Secure Endpoint to identify and block access from malware-infected devices.

With Duo Trusted Endpoints, you can:

- **Block attackers** – Allow only registered or managed devices to gain access to corporate apps and resources
- **Control device access** – Create and enforce a custom Trusted Endpoints policy to meet your organization's access security requirements when devices are not touching corporate networks
- **Cover BYOD and 3rd-party devices** – Safely grant access for unmanaged BYOD and third-party devices used by partners and contractors by adding them to your trusted device inventory
- **Mitigate risk** – Add an additional layer of verification and security with Trusted Endpoints when only weaker authentication options such as SMS or telephony are available

Duo and Cisco Secure Endpoint

Block compromised endpoints from accessing resources



Users use their devices to access applications

Cisco Secure Endpoint running on the device detects malware

Cisco Secure Endpoint notifies Duo about the infected device

Duo blocks that device from accessing apps

To experience Duo Trusted Endpoints, register for a free trial.