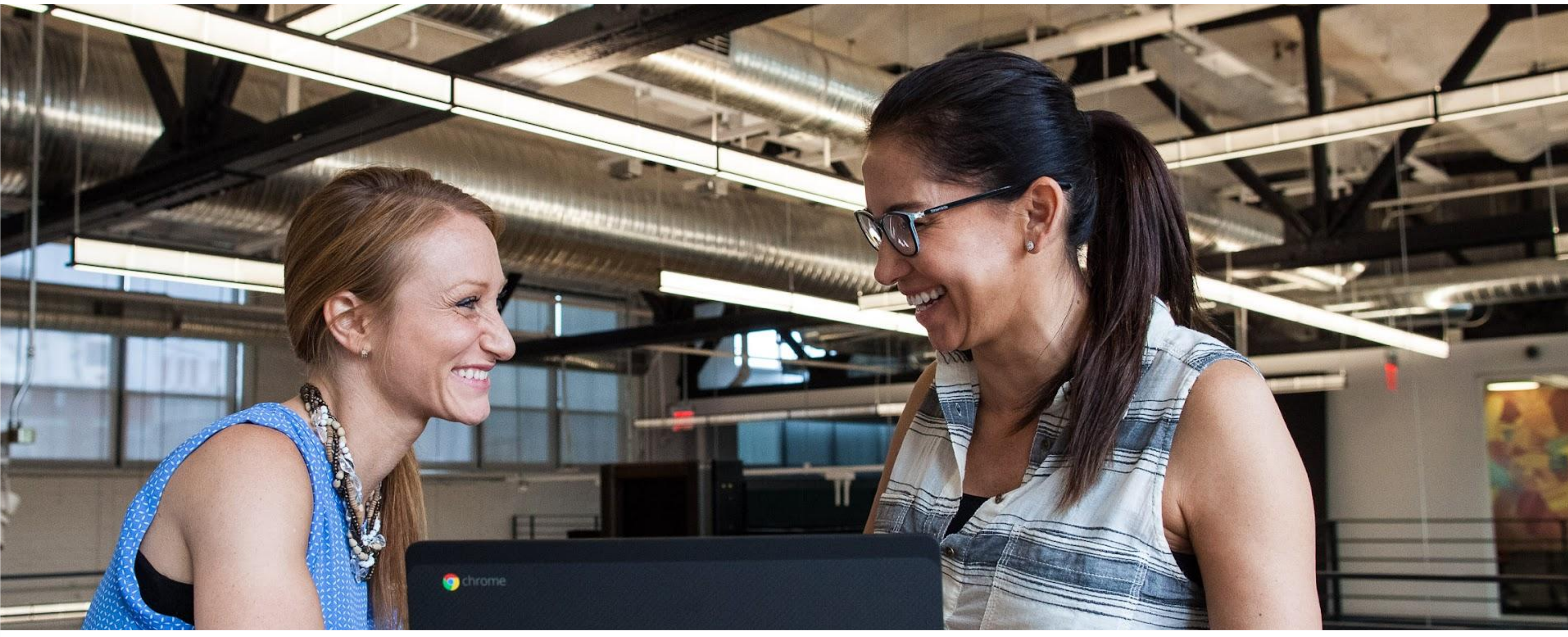
chrome enterprise

CISCO DUO

Cisco Duo Device Trust Connector Integration with Chrome Setup Guide

May 2024

Table of Contents



Chrome Device Trust Connector in Cisco Duo Overview

The Device Trust Connector is an integration between Chrome and a 3rd party IdP that provides attestation of the device identity without heavy weight integrations or agents.

Cisco Duo can use the signals to enforce Device Trust to increase security posture in Zero Trust architectures. Encrypted signals are delivered to Cisco Duo via a real-time HTTP header flow.

This document outlines the steps to enable and use the Chrome Device Trust Connector in Cisco Duo.

This feature is available for all licensed editions of Cisco Duo - Essentials, Advantage and Premier.

Requirements:

- **Licensed edition of Cisco Duo - Essentials, Advantage or Premier**
- **Chrome Enterprise Core or ChromeOS Enterprise/Edu Upgrade**
- **Chrome browser M109 or later**

What platforms are Device Trust Connector supported on?

✓ **Windows** ✓ **ChromeOS*** ✓ **Mac**

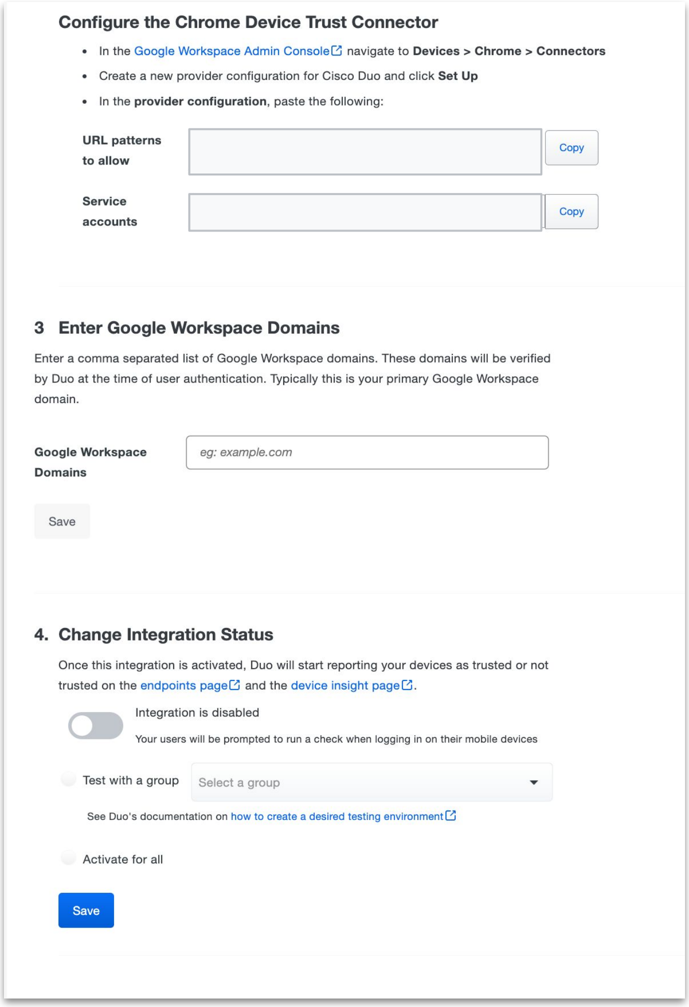
*ChromeOS M108 or later. Currently not available on ChromeOS Flex.

Setup

Enable the Chrome Device Trust Connector in the Cisco Duo Admin Panel

In order to set up the connection from Chrome to Cisco Duo, you will need to create or add it to an existing policy.

1. Log into the **Duo Admin Panel** and navigate to "**Trusted Endpoints**".
   - If this is your first integration, click the "get started" button at the bottom of the page.
2. On the "**Add Management Tools Integration**" page, select "**Chrome Device Trust Connector"** and then choose your supported OS from the dropdown menu and click the "add" button
   - Note that if you support multiple OS platforms, you will need to add the integration for each one.
3. In the following screen, in the section called "**Configure the Chrome Device Trust Connector**", copy the values in the "**URL patterns to allow**" and the "**Service account**" fields and save these values as you will need them in the following section.
4. Enter in your domain in the "**Google Workspace Domains**" field.
5. The integration is created in the "Disabled" state.
   - You'll turn it on when you're ready to apply your Duo Trusted Endpoints policy.
   - Turning on this integration will take precedence over any other active integration.



Configure the Chrome Device Trust Connector

- In the Google Workspace Admin Console navigate to **Devices > Chrome > Connectors**
- Create a new provider configuration for Cisco Duo and click **Set Up**
- In the **provider configuration**, paste the following:

URL patterns to allow		Copy
Service accounts		Copy

3 Enter Google Workspace Domains

Enter a comma separated list of Google Workspace domains. These domains will be verified by Duo at the time of user authentication. Typically this is your primary Google Workspace domain.

Google Workspace Domains: *eg: example.com*

Save

4. Change Integration Status

Once this integration is activated, Duo will start reporting your devices as trusted or not trusted on the endpoints page and the device insight page.

Integration is disabled

Your users will be prompted to run a check when logging in on their mobile devices

○ Test with a group: Select a group

See Duo's documentation on how to create a desired testing environment

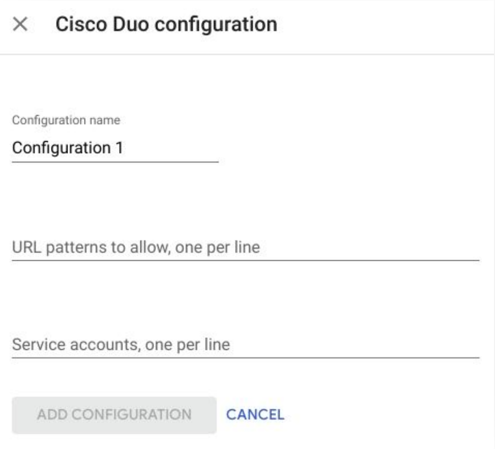
○ Activate for all

Save

Setup

Enabling Device Trust Connector in the Google Admin console

1. Go to the Google Admin console.
2. Go to **Devices > Chrome > Connectors.**
3. (If applicable) Accept the Connectors notification.
4. Hit the "**+ New Provider"** Configuration button.
5. Choose the Cisco Duo device trust connector provider and click "**Set Up".**
6. Provide a unique name for your configuration under "**configuration name**".
7. Enter the values from Step 3 of the previous section for the URL patterns to allow and the service account
8. Hit "**Add Configuration**".



✕ Cisco Duo configuration

Configuration name
Configuration 1

URL patterns to allow, one per line

Service accounts, one per line

Now you can apply this provider configuration to your desired organizational unit.

a. Choose your desired organizational unit on the tree UI widget to the left.
b. Scroll down to "**Device trust connectors**", use the radio buttons in this section to apply the appropriate configuration.
c. Hit "**Save".**

Setup

Enable the integration in the Cisco Duo Admin Panel

After creating the **Chrome Device Trust Connector Trusted Endpoints** integration, set the "Trusted Endpoints" policy to start checking for managed devices as users authenticate to Duo-protected services and applications.

1. When your trusted endpoints policy is applied to your Duo applications, return to the **Chrome Device Trust Connector Trusted Endpoints** integration in the Duo Admin Panel. The "Change Integration Status" section of the page shows the current integration status (disabled by default after creation). You can choose to either activate this integration only for members of a specified test group or groups, or activate for all users.
2. To enable the integration to require the device to be trusted, you need to apply to a existing or new policy. For more information about applying trusted endpoint policy to applications and groups, check out this page (Refer to the section called "Applying the Trusted Endpoints Policy to Applications and Groups")

Setup

Verify scenario

Assign the Cisco Duo authentication policy you just edited to an application, or confirm that it's already assigned to an app you can test.

2. Log into the application.

3. Confirm within the **Cisco Duo Admin Panel** authentication logs (Reports⟶Authentication Log) that recent successful access attempts to the protected application say "Trusted Endpoint verified by Google".

FAQ

What is Chrome Enterprise Core?

Chrome Enterprise Core offers a Chrome browser cloud management tool that provides the ability to manage Chrome browser from a single, cloud-based admin console, across all your Microsoft Windows, Apple Mac, Linux, iOS, and Android devices at no additional cost. **It is also a prerequisite** for setting up and managing the integration with Cisco Duo.

- Enforce 100+ Chrome policies for all users who open Chrome browser on a managed device. These are the same policies that can be managed with on-premise tools like Windows Group Policy.
- Users don't have to sign in or have Google Accounts to receive policies.
- Block suspicious extensions across your organization and do other common IT tasks.
- View reports on Chrome browsers deployed across your organization, including each browser's current version, installed apps and extensions, and enforced policies.

Follow these steps to roll out Chrome browser to your organization.

FAQ

How are managed browsers trusted?

The Chrome servers establish trust with managed browsers based on the Trust On First Use mechanism. When it detects that the Device Trust Connector is enabled, a managed browser will create an asymmetric key pair and upload the public key to be stored along with the browser's record in the Google Admin console. That public key will subsequently be used to validate signatures and establish trust with regards to the origin of a payload.

Notes on Keys

Keys are only used on Windows and Mac. The ChromeOS integration instead establishes trust using enterprise certificates stored on managed devices.

The "Clear key" operation can be useful for admins who are trying to unblock their users who, somehow, managed to lose their initial key.

FAQ

How can I clear a trusted key?

Admins with access to the Google Admin console can clear a trusted public key for a specific browser. This troubleshooting step can prove useful if a user is experiencing access issues which have the symptoms of a managed browser no longer having access to the trusted key pair.

The "Clear Key" action will simply delete the public key stored on the server for the corresponding browser. This will allow the user to restart the browser and have it upload its current public key to establish trust once again.

Key Revocation Supported Operating Systems

✓ Windows ✓ Mac

Clearing a Trusted Key

To clear a key, visit Chrome Enterprise Core and follow the steps:

1. Go to **Devices > Chrome > Managed browsers**.
2. Select the "Organizational Unit" where the browser(s) is located.
3. Select the browser with the key to be cleared.
4. Underneath the "Managed Browser" details box on the left hand side click "**Configure Key"**.
5. Select "**CLEAR KEY"**.

If the "Configure Key" is not clickable it is most likely because the key does not exist on the server.

FAQ

How do I unenroll a device?

To unenroll a managed device from Chrome browser cloud management navigate to this page for more information. To unenroll a ChromeOS device follow these steps.

Additional Resources

- Chrome Enterprise Core
- Chrome Device Management
- Learn More at Chrome Enterprise Help Center
- Learn More at Cisco Duo Help Center