chrome enterprise

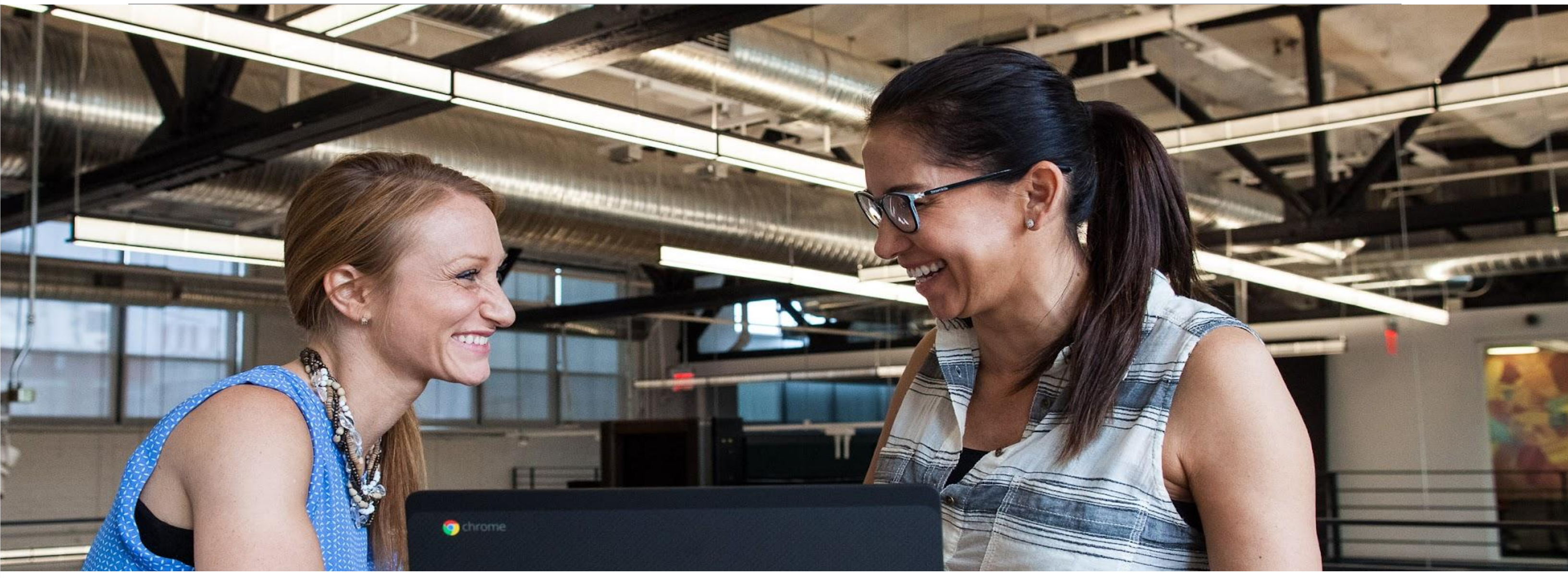
CISCO DUO

Cisco Duo Device Trust Connector Integration with Chrome Setup Guide

January 2025

chrome enterprise

Table of Contents



chrome enterprise

CISCO DUO

Chrome Enterprise Device Trust Integration with Cisco Duo Overview

The Device Trust Connector integration between Chrome Enterprise and Cisco Duo can confirm a device's legitimacy even if it is unmanaged by your enterprise.

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 agentless approach allows for the enforcement of a security baseline through Chrome Enterprise Premium on unmanaged endpoints protecting actions like uploads, downloads, copy/paste, printing, screenshots, and utilizing watermarking.

This document outlines the steps to enable and use the integration 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**
- **Access to the Google Admin Console**
- **Google Identity accounts**
- **A license or trial for Chrome Enterprise Premium (For Enhanced security features)**

What platforms are Device Trust Connector supported on?

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

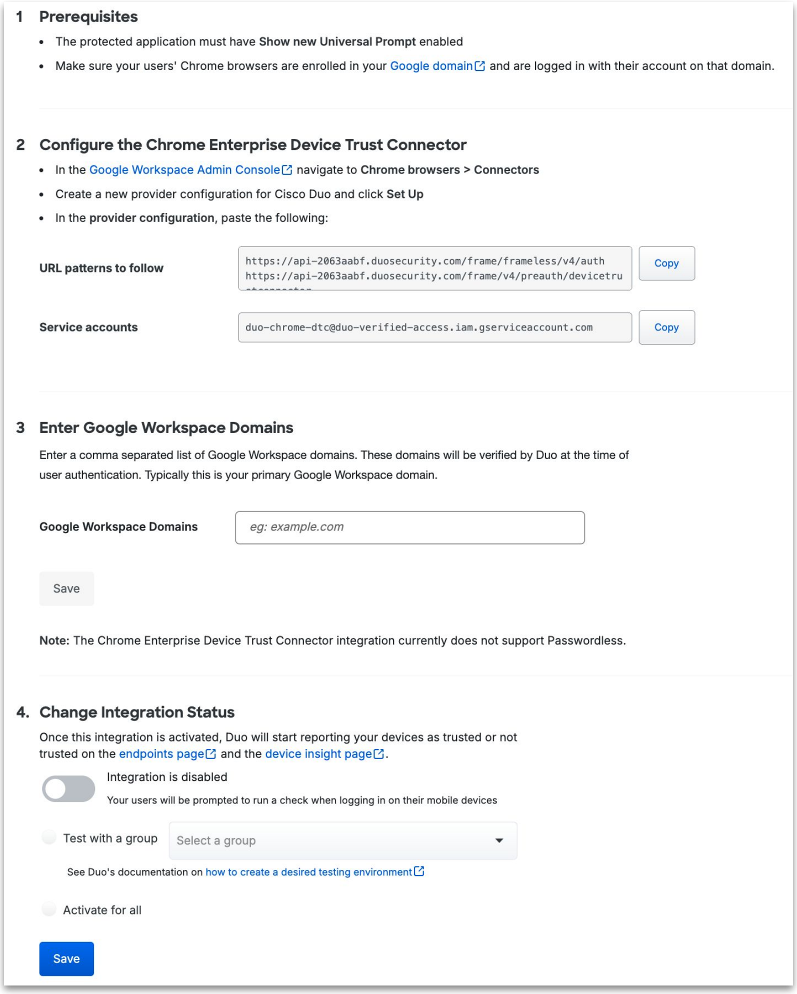
*ChromeOS M108 or later. Currently not available on ChromeOS Flex.

Setup

Enable Device Trust Connector in the Cisco Duo Admin Panel

In order to set up the connection from Chrome Enterprise 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 Enterprise Device Trust Connector”** and choose your supported OS from the dropdown menu and click the “add” button
   - Note: If you support multiple OS platforms, you need to add the integration for each one.
3. In the following screen, in the section called “**Configure the Chrome Enterprise 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.



1 **Prerequisites**

- The protected application must have **Show new Universal Prompt** enabled
- Make sure your users' Chrome browsers are enrolled in your Google domain and are logged in with their account on that domain.

2 **Configure the Chrome Enterprise Device Trust Connector**

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

URL patterns to follow

```
https://api-2063aabf.duosecurity.com/frame/frameless/v4/auth
https://api-2063aabf.duosecurity.com/frame/v4/preauth/devicetru
```

Service accounts

```
duo-chrome-dtc@duo-verified-access.iam.gserviceaccount.com
```

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*

Note: The Chrome Enterprise Device Trust Connector integration currently does not support Passwordless.

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

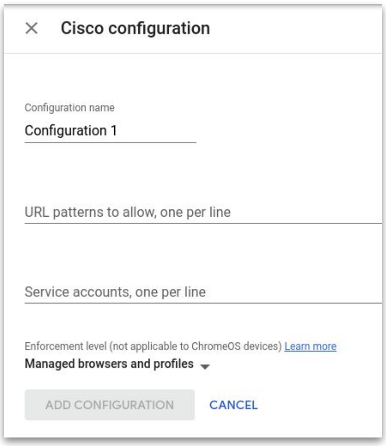
See Duo's documentation on how to create a desired testing environment

○ Activate for all

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 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. (Optional) Select how you want to apply the configuration—Managed Browsers Only, Managed Profiles Only, or both Managed Browser and Profiles.
8. Hit "**Add Configuration**".



Cisco configuration

Configuration name
Configuration 1

URL patterns to allow, one per line

Service accounts, one per line

Enforcement level (not applicable to ChromeOS devices) Learn more
Managed browsers and profiles

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 Enterprise 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 Enterprise 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.

1. Log into the application.
2. 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".

Setup

Options for enabling Chrome Enterprise Premium

To get the most out of Cisco Duo integration with Chrome browser, you need Chrome Enterprise Premium. Here's why:

- **Full DLP Coverage:** Chrome Enterprise Premium enables comprehensive Data Loss Prevention (DLP) for unmanaged endpoints when integrated with Cisco Duo.
  - This includes controlling actions like uploads, downloads, copy/paste, printing, and screenshots, as well as applying watermarks.
- **Enhanced Security:** Without Chrome Enterprise Premium, these enhanced security features won't apply, leaving your data potentially vulnerable.

Here's are your options:

- **Enable a Trial:** You can easily enable a trial of Chrome Enterprise Premium to test out these functionalities. Follow this guide to set-up a 60 day trial.
- **Existing License:** If you already have a Chrome Enterprise Premium license you can proceed directly to the next section.

FAQ

What is Chrome Enterprise Premium?

Chrome Enterprise Premium is a comprehensive security and management solution for businesses using Chrome browser. It builds upon the standard Chrome Enterprise offering by adding advanced features like enhanced data loss prevention (DLP), watermarking, and more. These features help organizations bolster their security posture, protect sensitive data, and streamline browser management, especially in today's increasingly cloud-centric and hybrid work environments.

For more information about how to set-up and test these protections in conjunction with the Cisco Duo integration, please refer to this setup guide for Chrome Enterprise Premium.

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.

Are both Google Identity users and enrolled devices supported?

Device trust connector supports both Google identity accounts and devices that are enrolled in Chrome enterprise core.

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

Will my users notice anything when this feature is enabled?

A consent dialog will pop-up for end users in certain management contexts (e.g. unmanaged devices). Devices that are enrolled in Chrome Enterprise Core for browser management will not see a pop-up or be required to sign into the browser for the integration to function. A managed profile will not be created if end users do not accept the consent dialog. Please note that even if the device is managed by MDM, the pop-up will still show if the browser is not enrolled in Chrome Enterprise Core.

Any applications that I should be careful of integrating?

If you set up Google Workspace using Duo's conditional access policies to restrict access it can cause issues where the end user won't be able to login to the Chrome Profile with a managed user account. The solution for this is for admins to protect Workspace via Chrome Enterprise Premium, and then you can protect other apps via the Duo's conditional access. We are working on another feature which helps alleviate this issue in the near future.

Will I get all device Signals for Managed Profiles?

Yes. All device signals will be available for Managed Profiles/user accounts.

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

January 2025