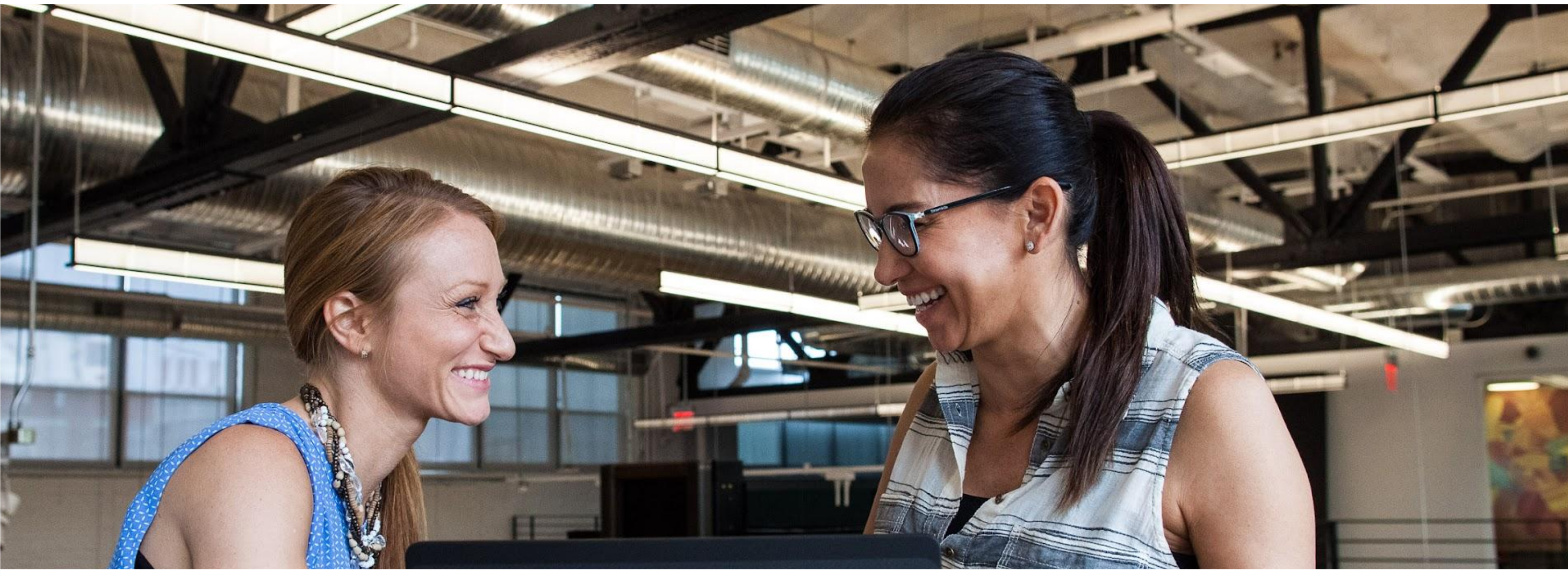
chrome enterprise

zscaler™

Zscaler Device Trust Integration with Chrome Setup Guide

January 2025

Table of Contents



Chrome Enterprise Device Trust Integration with ZPA Overview

The Device Trust integration between Chrome Enterprise Premium and Zscaler Private Access can confirm a device's legitimacy even if it is unmanaged by your enterprise.

- 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.
- Furthermore, access to private web applications is securely handled through Zscaler Private Access (ZPA).
- Encrypted signals are transmitted to ZPA via a real-time HTTP header flow.

This document explains the steps to enable and utilize this integration in ZPA.

This feature is available for all licensed editions of Zscaler Private Access.

Requirements:

- **Zscaler Private Access**
- **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**

What platforms are Device Trust integration supported on?

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

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

Setup

Options for enabling Chrome Enterprise Premium

To get the most out of Zscaler Private Access (ZPA) 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 ZPA.
  - 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:

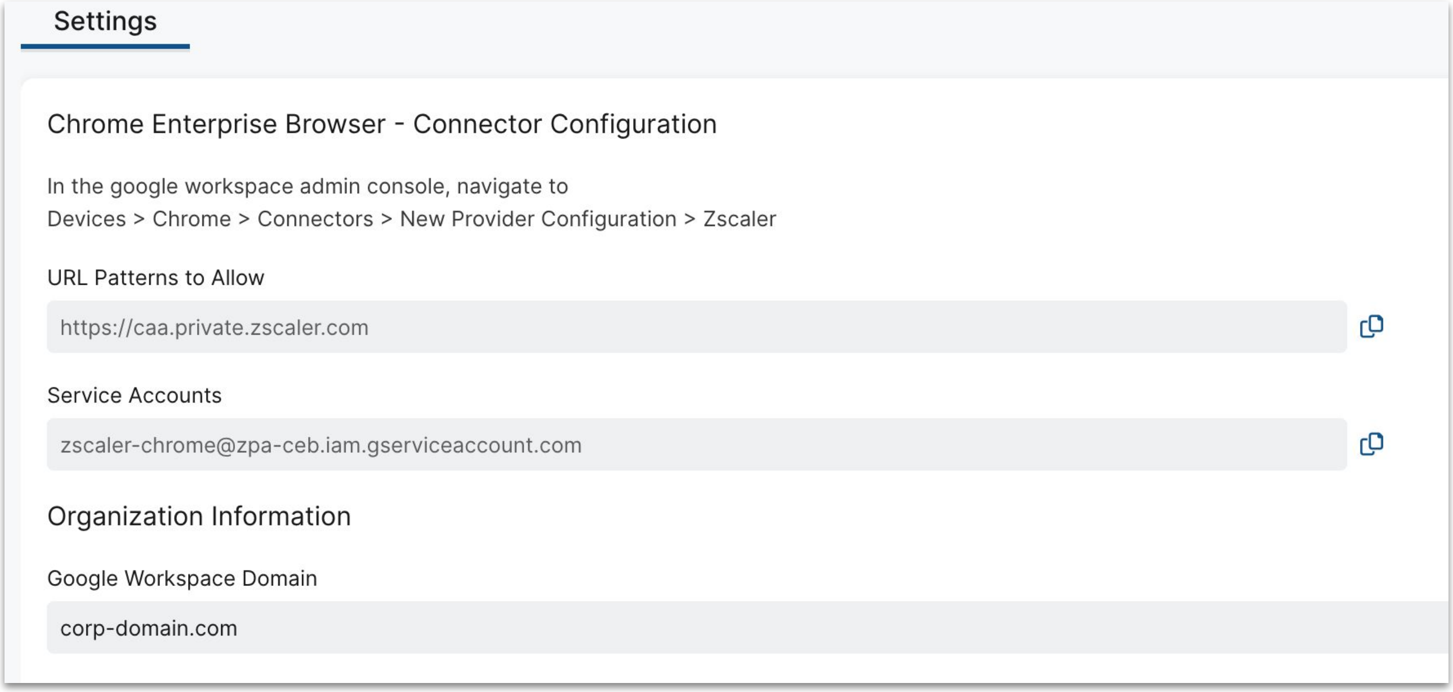
- Enable a Trial: You can easily enable a trial of Chrome Enterprise Premium to test out these functionalities. Follow this guide to setup a 60 day trial.
- Existing License: If you already have a Chrome Enterprise Premium license you can proceed directly to the next section.

Setup

Setup the Chrome Enterprise Device Trust integration in the Zscaler Admin Portal

In order to set up the connection from Chrome Enterprise to ZPA, you will need to first configure your domain on the Zscaler Admin Portal.

1. Log into the **Zscaler Admin Portal** and navigate to "**Configuration & Control > Chrome Enterprise Browser > Settings**".
2. On the "**Settings**" page, copy the values in the "**URL Patterns to Allow**" and the "**Service Accounts**" fields and hold onto these values as you will need them in the following section.
3. In the field called "**Google Workspace Domain**", enter your Google Workspace domain as per your organization's requirements and hit the **Save** button.



Settings

Chrome Enterprise Browser - Connector Configuration

In the google workspace admin console, navigate to
Devices > Chrome > Connectors > New Provider Configuration > Zscaler

URL Patterns to Allow

https://caa.private.zscaler.com

Service Accounts

zscaler-chrome@zpa-ceb.iam.gserviceaccount.com

Organization Information

Google Workspace Domain

corp-domain.com

Setup

Enabling Device Trust integration in the Google Admin console

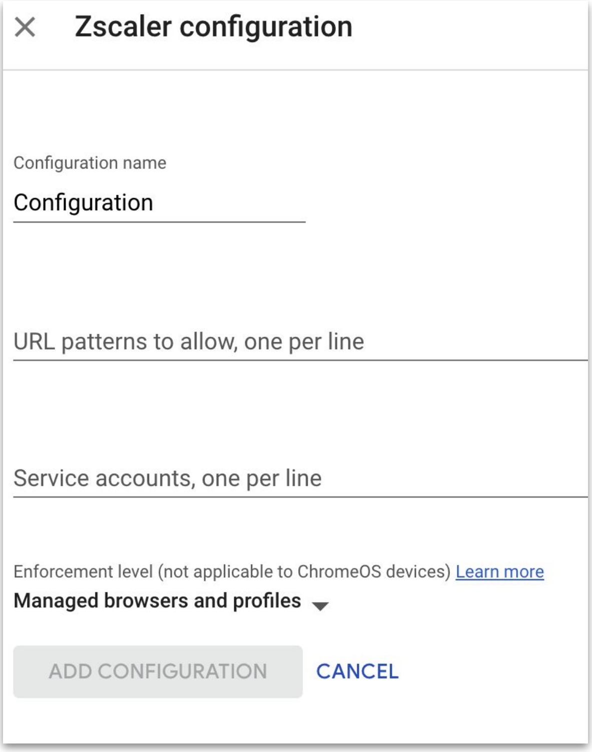
1. Go to the Google Admin console.
2. Go to **Devices > Chrome > Connectors.**
3. (If applicable) Accept the Connectors notification.
4. Hit the **"+ New Provider"** Configuration button.
5. Choose the Zscaler Device Trust integration provider and click **"Set Up".**
6. Provide a unique name for your configuration under **"configuration name**".
7. Enter the values from Step 2 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**".

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 integrations**", use the radio buttons in this section to apply the appropriate configuration.

c. Hit "**Save**".



Zscaler configuration

Configuration name: Configuration

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

Setup

Finishing the configuration in the Zscaler Admin Portal

After configuring the **connector settings in the Google admin console** you can now configure an access policy with Chrome Enterprise Browser as a criteria (Access policies can be found under Policy ⟶ Access Policy) so that ZPA restricts access only to Managed Chrome Browsers (and/or Profiles) for your configured domain.

1. You can do this by creating a new access policy or editing an existing policy. Scroll down to the **Criteria** section of the **Add Access Policy (for a new access policy) or Edit Access Policy (for an existing access policy)** page and click on **Add Criteria**.

2. Select the **Chrome Enterprise Browser** Criteria from the list of options.

   - Make sure to move the slider of the **Chrome Enterprise Browser** criteria such that it turns green with a check mark to start checking for device signals as users authenticate to ZPA-protected services and applications.

   - You can choose to either apply the **access policy** only for specific App Connector Groups and Server Groups, or activate for all App Connector Groups. For more information about Access policies, check out this page

Setup

Verify that access policy is applied

Confirm that the **Access Policy** is assigned to an application you can use to test.

1. Log into the application.
2. Confirm within the **Zscaler Admin Portal** User Activity Logs (Analytics→Diagnostics) that recent successful access attempts contain the **Chrome Enterprise Browser** device signals in the event details (Under **User Metadata**).

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 setup and test these protections in conjunction with the ZPA 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 Zscaler Private Access.

- 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 integration 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 integration 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 your Identity Provider'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 private apps via ZPA'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
- Chrome Enterprise device trust connectors
- ZPA and Chrome Browser Product Documentation