chrome enterprise

omnissa™

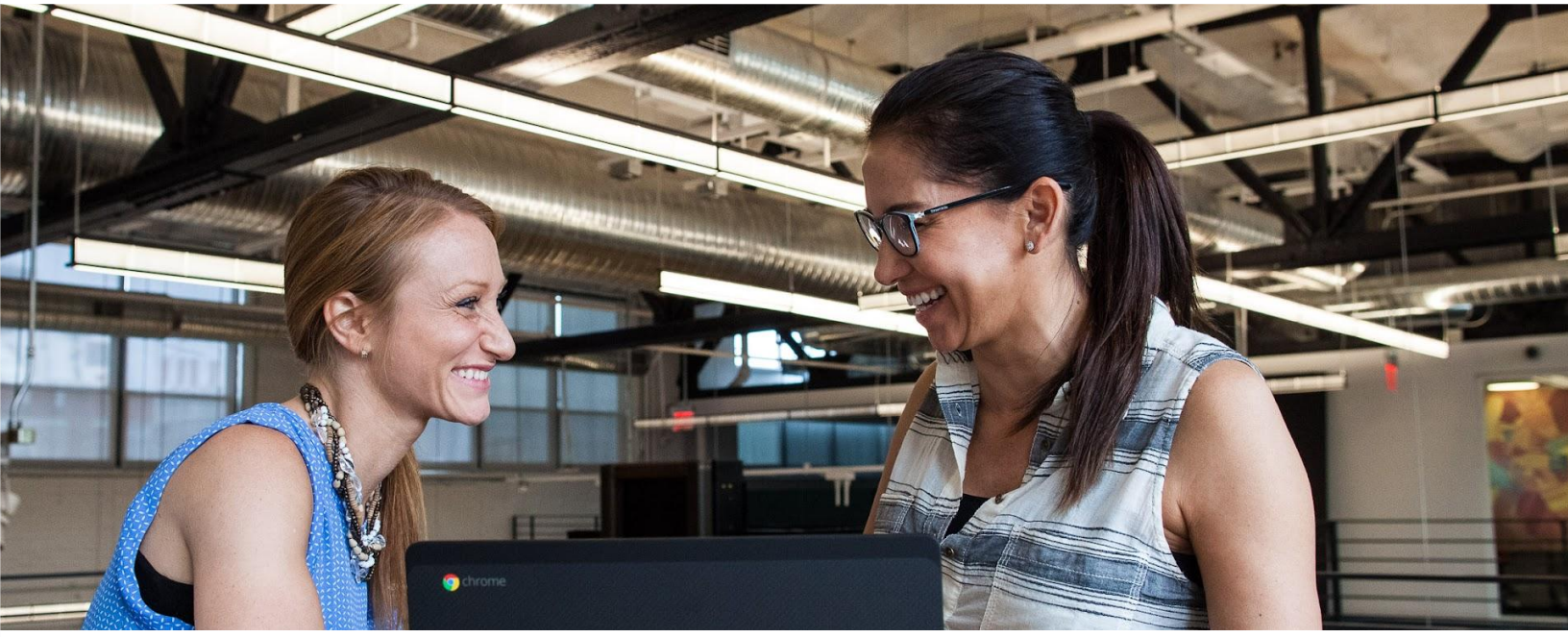
Omnissa Device Trust Integration with Chrome Setup Guide

November 2024

chrome enterprise

omnissa™

Table of Contents



chrome enterprise

omnissa™

Chrome Enterprise Device Trust Integration with Omnissa Access Overview

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

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

This document outlines the steps to enable and use the integration in Omnissa Access.

This feature is available for all licensed editions of Omnissa Access.

Requirements:

- **Omnissa Access version 24.10+**
- **Chrome Enterprise Core or ChromeOS Enterprise/Edu Upgrade**
- **Chrome browser M109 or later**

What platforms are Device Trust integration supported on?

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

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

chrome enterprise

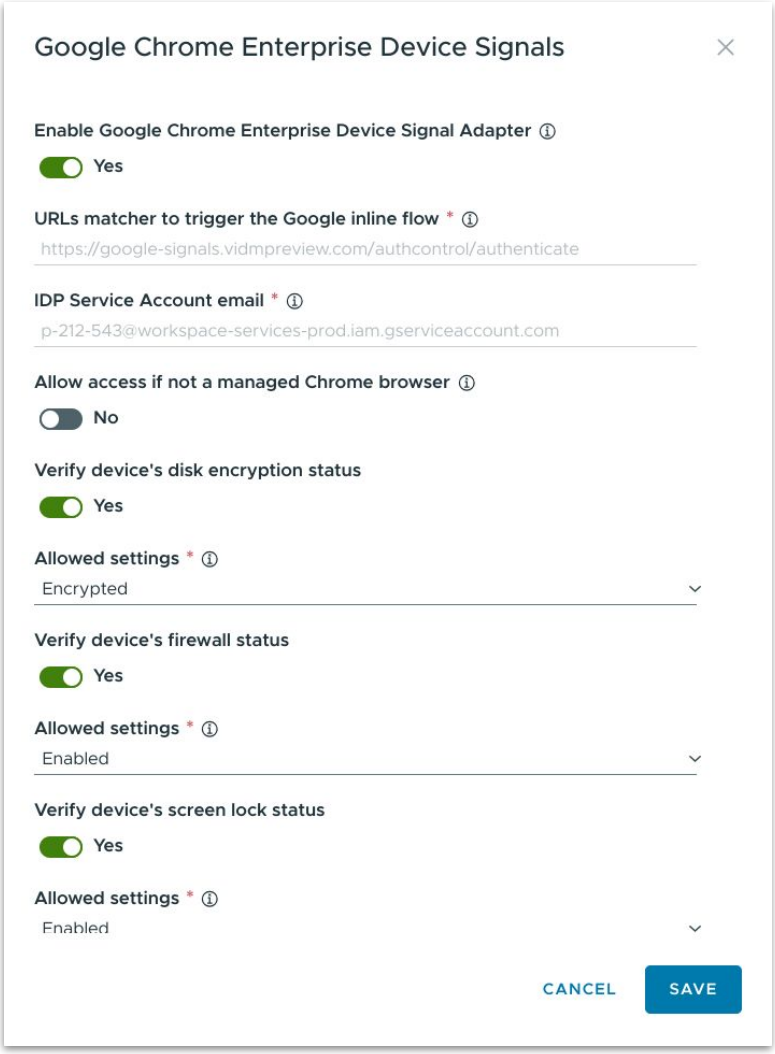
omnissa™

Setup

Enable the Chrome Enterprise Device Trust integration in the Omnissa Access Console

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

1. Log into the **Omnissa Access Console** and navigate to "**Integrations**".
   - If this is your first integration, click the "get started" button at the bottom of the page.
2. On the "**Authentication Methods**" page, select "**Google Chrome Enterprise Device Signals**" and then click the "Configure" button
3. In the following screen, in the section called "**Google Chrome Enterprise Device Signals**", copy the values in the "**URLs matcher to trigger the Google inline flow**" and the "**IDP Service Account email**" fields and save these values as you will need them in the following section.
4. Modify the other settings as per your organizations requirements.
5. Create the integration in the "Enabled" state.
   - You'll have to associate it with your Identity Provider before you add it to your access policy.



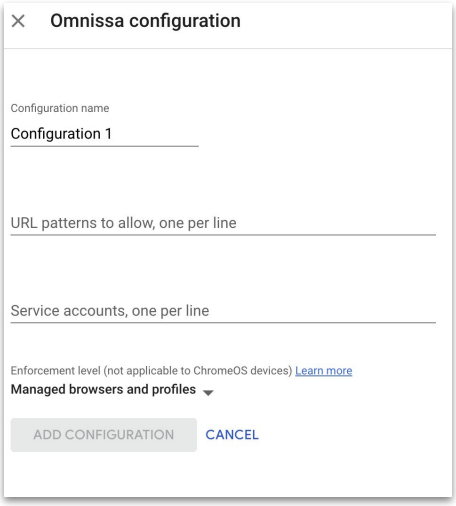
chrome enterprise

omnissa™

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 Omnissa 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 3 of the previous section for the URL patterns to allow and the service account
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**".

chrome enterprise

omnissa™

Setup

Enable the integration in the Omnissa Access Console

After creating the **Google Chrome Enterprise Device Signals** authentication method, associate it with an existing Identity Provider (Authentication methods can be selected in the Identity Provider settings under Integration → Identity Providers) so that the authentication method is available to an access policy containing the Identity Provider.

1. After associating the **Google Chrome Enterprise Device Signals** authentication method with an Identity Provider, set it as a policy rule in an "Access" policy (Under Resources → Policies) to start checking for device signals as users authenticate to Access-protected services and applications.

2. You can choose to either apply the **Google Chrome Enterprise Device Signals** enabled "Access" policy only for members of a specified test group or groups, or activate for all users. For more information about applying an Access policy to user groups, check out this page

chrome enterprise

omnissa™

Setup

Verify scenario

Confirm that the **Google Chrome Enterprise Device Signals** authentication method enabled Access policy is already assigned to an user you can use to test.

1. Log into the application.
2. Confirm within the **Omnissa Access Console** audit events report (Monitor→Reports) that recent successful access attempts say “success”:”true” in the event details.

chrome enterprise

omnissa™

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 Omnissa 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.

chrome enterprise

omnissa™

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

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 Omnissa'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 Omnissa'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.

chrome enterprise

omnissa™

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.

chrome enterprise

omnissa™

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 Omnissa Product Documentation