chrome enterprise

okta

Okta Device Trust Connector Integration with Chrome Setup Guide

July 2024

chrome enterprise

okta

Table of Contents

chrome enterprise

okta

Device Trust Connector Overview

The Device Trust Connector is an integration between Chrome Enterprise and a 3rd party IdP that provides attestation of the device identity and enables access to context aware signals.

Okta can use the signals to implement Context Aware Access (CAA) for use in Zero Trust architectures. Encrypted signals are delivered to Okta via a real-time HTTP header flow.

This document outlines the steps to follow to enable and use the integration in Okta.

Note: This integration may require a certain license type in Okta. Please refer to this document for additional information.

chrome enterprise

okta

Setup

Enable the Chrome Device Trust Connector in the Okta Admin Console

In order to setup up the connection from Chrome Enterprise to Okta, a service account will need to be created for you. Navigate to ***Security > Device Integrations*** and select ***Add endpoint integration***.

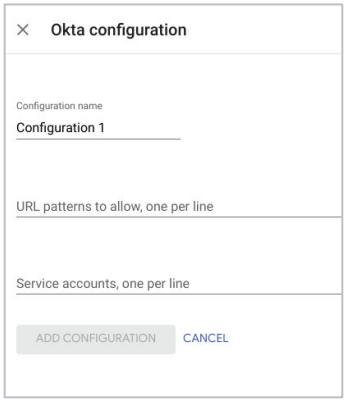
1. Select ***Chrome Device Trust*** and the OS platforms for which you wish to enable the integration.
2. Copy the values in the ***URL patterns and Service account*** fields on the integration page. These values are unique to your tenant and will be used to link Okta to your Google Admin console.

chrome enterprise

okta

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 license agreement for using Connectors.
4. Hit the ***+ New Provider*** Configuration button.
5. Choose the Okta device trust connector provider and click ***Set Up.***
6. Provide a unique name for your configuration under “configuration name”.
7. Input the URL and service account information provided by your Okta contact.
8. Hit ***Add Configuration.***



9. 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.***

chrome enterprise

okta

Add Chrome Device Trust Connector in Okta Admin Console

1. **Create a Device Assurance policy for ChromeOS**
   a. Navigate to ***Security > Device Assurance Policies*** and select ***Add a policy.*** Select ChromeOS.
   b. Configure the device attributes in the policy editor and hit save.
2. **Create a Device Assurance policy for Managed Chrome Browser on Windows/macOS**
   a. Navigate to ***Security > Device Assurance Policies*** and select ***Add a policy.*** Select Windows or macOS.
   b. Select Google as your Device attribute provider
      i. Note: If you select both Okta and Google as your providers, for any signals that overlap between the providers (e.g. OS version), the source of truth will be Okta.
   c. Configure the device attributes in the policy editor and hit save.
3. **Add device assurance to an authentication policy**
   a. In the Admin console, go to ***Security > Authentication policies.***
   b. Select a policy and click **Add Rule** to add a new rule for device assurance. To add device assurance to an existing policy rule, select the policy rule you want to modify, and then click ***Edit.***
   c. For **AND** ***Device assurance policy is,*** select ***Any of the following device assurance conditions,*** and then enter the name of a device assurance you have previously created.
      i. You can add multiple platform-specific device assurance policies.
      ii. If you add multiple sets of device assurance attributes to the same rule, they're OR conditions.
      iii. If the rule has other conditions, all of the conditions defined for the rule must be met for the rule to be applied.
   d. Specify any additional conditions and what should be done if the conditions are met.
   e. Click ***Create Rule*** or ***Save*** to save your changes.

chrome enterprise

okta

Verify setup

1. Assign the Okta authentication policy you just edited to an application, or confirm that it's already assigned to an app you can test.
2. Log in to the application.
3. Confirm in Okta system logs that Chrome Device Trust signals are in the recent access attempt. Ensure the CHROME_DTC appears as a Device Integrator object in the authentication success event created for your test access.

chrome enterprise

okta

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.

chrome enterprise

okta

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 Okta's 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 Okta's access policies. 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

okta

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

- Windows
- Mac

Clearing a Trusted Key

To clear a key visit Cloud Browser Cloud Management 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

okta

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.

What platforms is Device Trust Connector supported on?

- Windows
- ChromeOS*
- Mac

*Currently not available on ChromeOS Flex

Additional Resources

- Chrome Browser Cloud Management
- Chrome Device Management
- Learn More at Chrome Enterprise Help Center
- Learn More at Okta Help Center