

Trellix DLP Endpoint Integration for Chrome Enterprise Setup Guide

April 2024



Table of Contents

Local Content Analysis Connector Overview	03
Setup	05
Get access to the Google admin console	05
Create a test Organizational Unit and enroll test devices into CBCM	06
Enabling Local Content Analysis Connector in the Google Admin Console	08
Verify that the policies are applied on your test machine	10
Setup Trellix DLP Endpoint Agent	10
Platform Supported	11
Additional Resources	11

Local Content Analysis Connector Overview

Many enterprises wish to extend Trellix DLP Endpoint protection to monitor Chrome browser usage for data exfiltration and apply allow/block controls based on their DLP policies.

Existing extension based methods for allowing DLP systems to interface with Chrome need continual review. Version upgrades can cause incompatibility, resulting in instability and performance issues. In addition, these solutions are less able to solve advanced DLP use cases. The integration with Chrome solves many of these issues.

This document outlines the steps to follow to enable and use the Chrome Local Content Analysis connector in Trellix.

Requirements:

- **Trellix DLP Endpoint Version 11.11 or later**
- **Chrome Browser M123 or later**
- [Chrome Browser Cloud Management](#)

Key Use Cases

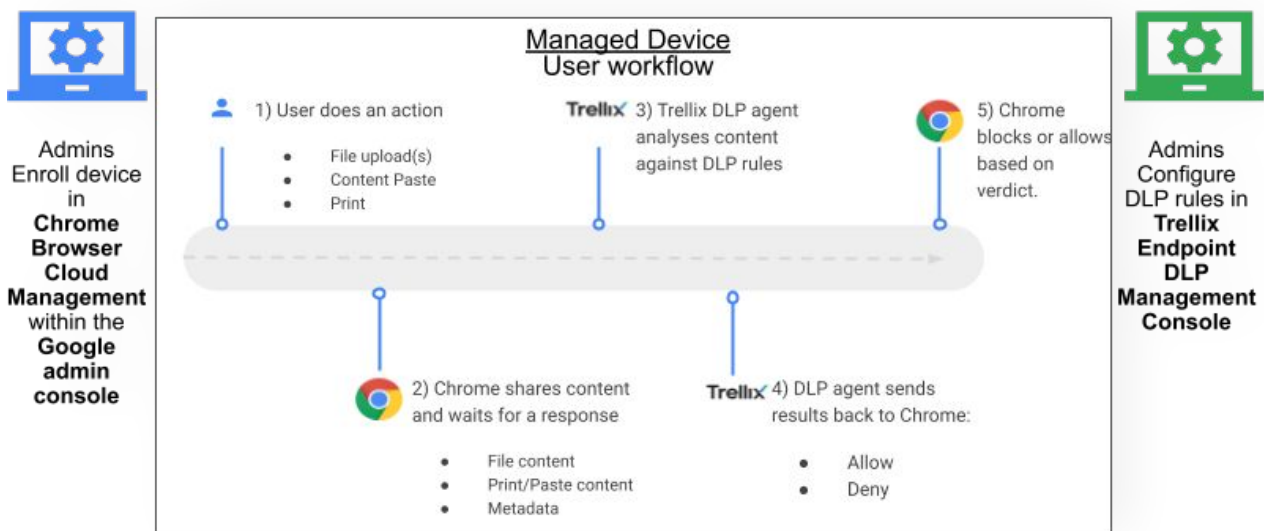
- User uploads files containing sensitive data in Chrome by browsing to the file.
- User uploads a file containing sensitive data in Chrome by dragging & dropping it into the page.
- User uploads files containing sensitive data in Chrome by Ctrl +C and Ctrl + V into the page.
- User pastes content into a page in Chrome from the clipboard.
- User prints a page containing sensitive data in Chrome via File->Print, Right Click + Print, Ctrl+P and Ctrl+Shift+P

Benefits

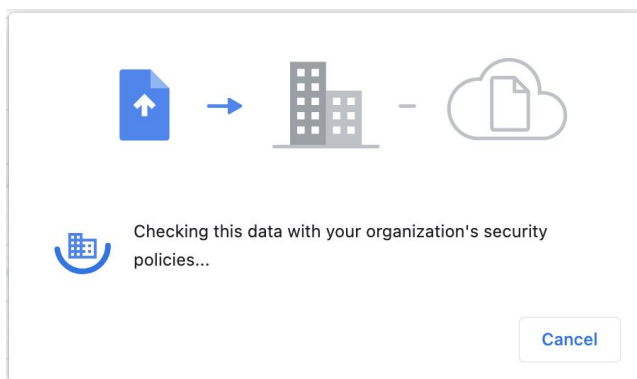
- Reduced risk of compatibility issues or breaks in DLP monitoring
- Shortened testing cycles in the customer environment
- Enhanced coverage for previously unsupported use-cases
- Improved browser performance and stability for end users due to the native integration

Local Content Analysis Connector Overview

Below is an overview of the solution:



When the user performs an operation such as File Upload, Clipboard paste or Print within Chrome, Chrome communicates the user action and the content (along with some metadata) to the Trellix DLP agent. Chrome then waits for a verdict from the service. During this time, Chrome freezes the tab and displays an appropriate UI to the user. Note this dialog is only shown if the scan tasks take more than 1 second.



Trellix DLP Agent analyzes content against DLP Rules and generates a verdict. If the Verdict is 'Block' or 'Warn', the agent will show a popup to the end user with an appropriate message.

The agent will also communicate this verdict with Chrome. If Chrome receives an "Allow" verdict from the agent, it will proceed to let the user complete the operation. If the verdict is 'Block' it will prevent the user from completing the desired operation.

Setup

Get access to the Google admin console

[Chrome Browser Cloud Management](#) is a no cost solution to manage Chrome browser. Having your device enrolled into this centralized console provides the connection to the Trellix DLP Endpoint integration. Gaining access to Chrome Browser Cloud Management is as follows:

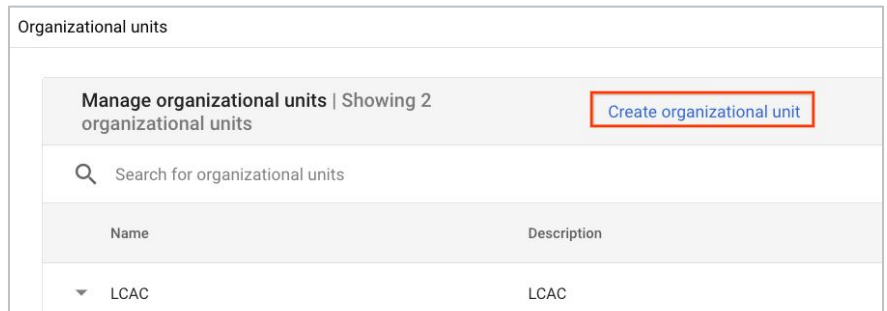
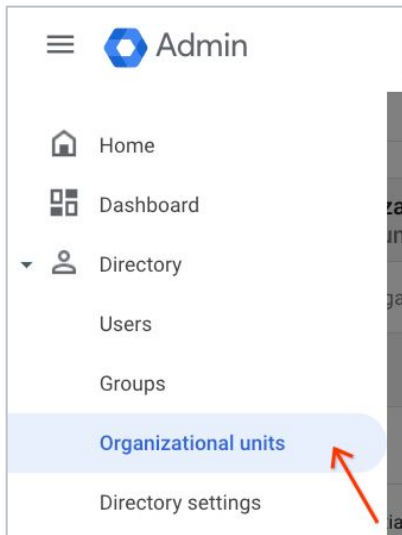
- **Non-Google Workspace Users:**
 1. You can use [this signup flow](#), which requires a business email address to sign up.
 - Note that there is no cost to CBCM.
 2. You'll get a verification email that will give you access to the admin console.
 3. Follow the steps in the wizard to enable CBCM for your account
- **Google Workspace Users:**
 1. Use a super admin account to log into <https://admin.google.com/>
 - To check if your account has “super admin” privileges, go to Directory > Users
 - Click the account name
 - The information is displayed under the “Admin roles and privileges” section
 2. Follow the steps in this guide under the section “[Add a Chrome Browser Cloud Management subscription](#)” to enable CBCM in your environment.
 - Note that there is no cost to enable CBCM.

Once you have your console setup or have access to an existing console, please refer to steps 1-3 in [the guides section](#) in the Google Admin Console to help you with verifying your domain, setting up Organizational units and enrolling your test machines in the console. More details on enrolling the test devices is located in the following section.

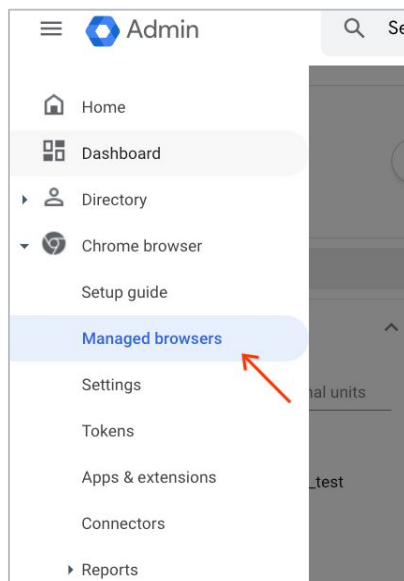
Setup

Create Organizational Unit(s) and enroll devices into CBCM

- 1 Create an Organizational Unit that you will use to enroll your devices by going to **Menu > Directory > Organizational Units** and click the **“Create organizational unit”** link to create a new one.
 - a This will make sure that the settings only apply to the machines enrolled in that Organizational Unit, so it will not affect any other machines.



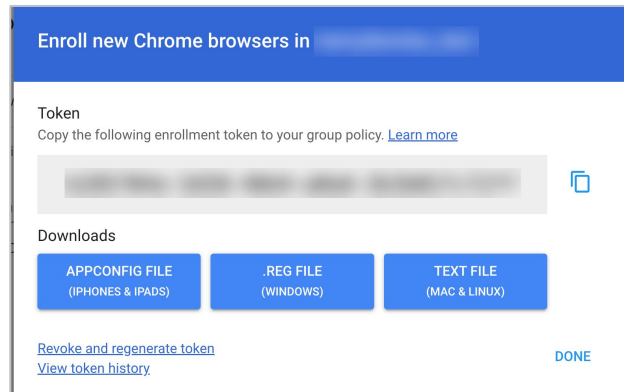
- 2 To enroll a machine in the Organizational Unit that you just created in the previous step go to **Menu > Chrome browser > Managed browsers**.



Setup

Create Organizational Unit(s) and enroll devices into CBCM

- 3 With the Organizational Unit that you created in step 1 selected, at the top, click the **Enroll** link.
 - a You'll see a token value appear. Click on the ".REG FILE" button to download a .reg file that will enroll your test machine.

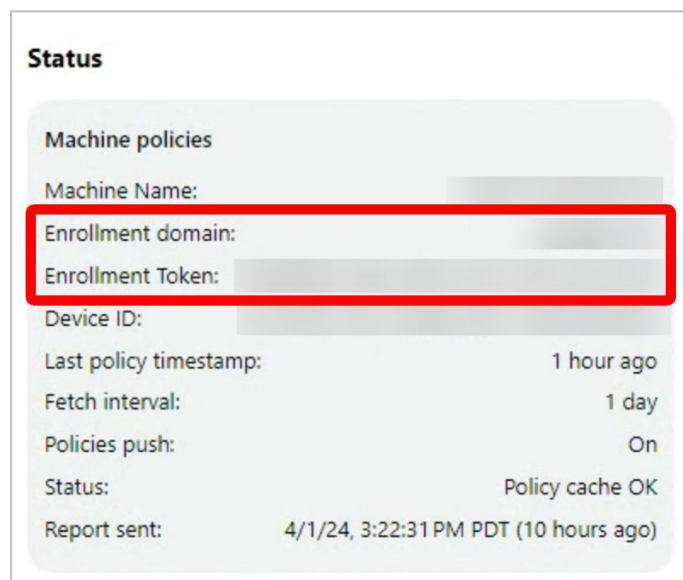


- 4 Execute the registry file on the Windows device you wish to enroll in the console.
 - a Please make sure Chrome is not running and that you have the rights needed to add the key as an administrator.
 - b Refer to [this Help Center article](#) for alternate ways to enroll your Windows device into CBCM.

- 5 Launch Chrome. Chrome should now enroll itself into CBCM.

- 6 You can use your Admin console to confirm enrollment. Steps described [here](#).

- 7 On the client side, you can verify whether your browser is enrolled into CBCM by typing **chrome://policy** into a new tab. You should see the token value from step 3 and see your domain present.












Setup

Enable Local Content Analysis Connector in the Google Admin console

Note: Make sure that your DLP Agent is installed and set up correctly on your enrolled Windows device before following the steps below.

- 1 Go to the [Google Admin Console](#).
- 2 Go to Menu > **Chrome Browser** > **Settings**
- 3 Filter for the word 'connectors' and select Category contains and you should see a section titled "**Chrome Enterprise connectors**"
- 4 **(First time users only)** Select Allow users to enable Enterprise Connectors from the dropdown menu.
- 5 **(First time users only)** Agree to the Connectors disclosure, if applicable.
- 6 **(First time users only)** Click "Save" on the upper right corner
- 7 Click the "**Edit in legacy view**" link.

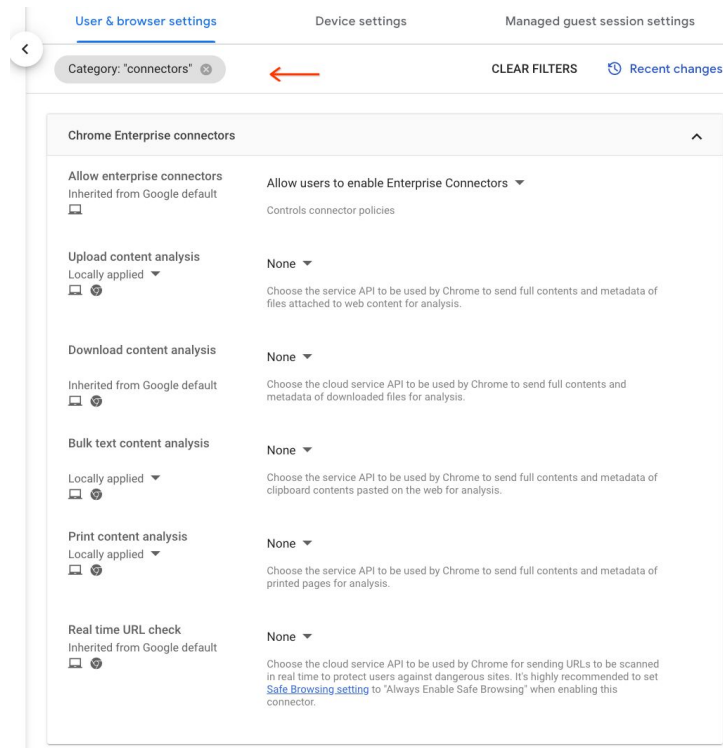
Chrome Enterprise connectors			
Setting	Configuration	Inheritance	Supported on
Allow enterprise connectors	Allow users to enable Enterprise Connectors	Google default	   iOS
Upload content analysis	Edit in legacy view	Locally applied	   iOS
Download content analysis	Edit in legacy view	Google default	   iOS

Continue on next page

Setup

Enable Local Content Analysis Connector in the Google Admin console

- 9 Filter for the word “connectors” and select Category contains.



- 10 Select “Trellix” from the dropdown menu. Currently supported functions are:
- Upload content analysis
 - Bulk text content analysis
 - Print content analysis
 - Hit **Add Configuration**.

- 11 Click “Save” again on the upper right corner

Setup

Verify that the policies are applied on your machine

On the machine(s) that you enrolled, launch Chrome browser and type in **chrome://policy** in the address bar. Verify the following:

- 1 The domain and token value match your Google Admin console
- 2 The token value for the Organizational Unit that you enrolled in the machine where you applied the Chrome Enterprise connector settings.
- 3 The following policies are present in the policy list and when you expand out the setting the service provider is listed as : "trellix".
 - OnBulkDataEntryEnterpriseConnector
 - OnFileAttachedEnterpriseConnector
 - OnPrintEnterpriseConnector

Setup Trellix DLP Endpoint Agent

Windows endpoint devices are required to have latest version of Trellix DLP Endpoint for Windows v11.11.




Please details refer to [this documentation](#).

Platform Supported

Chrome Enterprise Connector to Trellix DLP Endpoint is currently supported on:

-  Windows

Additional Resources

-  [Chrome Browser Cloud Management](#)
-  [Learn More at Chrome Enterprise Help Center](#)
-  [Learn More at Trellix Support Center](#)