

Chrome Enterprise Premium Trial Guide

October 2025



Table of Contents

Chrome Enterprise Premium Overview	03
Define your success criteria for Chrome Enterprise Premium	04
Sample Success Criteria for Chrome Enterprise Premium	05
Setup Access for Chrome Enterprise Premium	06
Prepare your Test Environment	07
Enable Cloud Identity & Chrome Enterprise Core	08
Create a Chrome Enterprise Management Role	09
Create a Organizational Unit Structure	10
Enroll Test Browsers and Create Test Users	11
Enable Chrome Enterprise Premium Connector Settings	12
Deploy Required Browser Extensions	13
(Optional) Set up Device Trust Connector	14
Start a Trial of Chrome Enterprise Premium	15
Use cases for Chrome Enterprise Premium - Managed browsers	16
Use cases for Chrome Enterprise Premium- Threat and Data Protection	17
Use cases for Chrome Enterprise Premium- Access Control	18
Use cases for Chrome Enterprise Premium- Investigation and Third Party Integrations	19
Troubleshooting	20
FAQ	24
Additional Resources	25

Use Chrome as a Secure Enterprise Browser

Chrome Enterprise Premium Overview

Secure enterprise browsing is the [emerging standard](#) for protecting corporate data while enabling your users to work securely on the web from anywhere on any device. [Chrome Enterprise Premium](#) provides:

- Configurable data loss prevention
- Real-time phishing, malware and sandboxing protections
- Controls to manage access to critical applications with least privilege access

This guide will provide you with the steps to set up a secure enterprise browser for user profiles and device based management. It will also include steps for setting up a trial (if needed) and enabling Chrome Security Insights to conduct a no-cost security review of possible risky browser activity in your enterprise.

Requirements (covered in this guide):

- [Chrome browser](#) installed on users' devices
- Access to a [Google Admin Console](#)
- Access to a [Google Cloud Console](#)
- Devices enrolled into [Cloud Management](#) and Google Cloud Identity licenses for users to be managed
- A license or a 60-day trial for Chrome Enterprise Premium



Define the Scope of your Proof of Value

Define your success criteria for Chrome Enterprise Premium

Chrome Enterprise Premium offers a variety of features to address common use cases in enterprises. When running the trial of Chrome Enterprise Premium, it is important to outline the scope of your success criteria. Each section of the guide can be tailored to protect your corporate data located in the following locations:

- Corporate Data within your SaaS Applications
- Assets located within Private Web Applications in Google Cloud Platform
- Data stored within private web applications in other clouds or on-premises

You also need to define the types of devices and users that require access to this data:

- Fully managed corporate users on company devices
- Corporate users, contractors, partners on unmanaged devices

Based on these aspects, you can refer to specific sections of this guide to maximize the benefits of your 60-day trial of Chrome Enterprise Premium. Use the sample criteria provided in the following section as a reference.



Select the use cases for your Proof of Value

Sample Success Criteria for Chrome Enterprise Premium

Control Category	Test Use Case	Desired Outcome
Managed Browser / Profile	A. Managed Devices (via Browser) B. Unmanaged Devices (via Profile) C. Reporting and Auditing D. Password Reuse E. Extension Control	A. Require managed device to meet security standard for app access B. Deliver a managed browser experience on unmanaged devices C. Report on activity across the entire fleet of devices in a single window D. Control the reuse of old/weak passwords E. Protect users from installing unapproved extensions
Data Protection	A. Upload Restrictions B. Download Restrictions C. Copy/Paste Control D. Print Control E. Web/URL Filtering F. Optical Character Recognition G. Watermarking H. Screenshot / screen-share protection I. Data Masking	A. Prevent sensitive data being uploaded to sites B. Prevent sensitive data from being downloaded to device C. Prevent sensitive data transfer going to/from Chrome Profile, Incognito, other apps D. Prevent printing of sensitive data E. Control what URL domains and categories can be accessed F. Analyze images and PDFs for sensitive data G. Overlay sensitive sites with Watermarks to discourage data exfiltration H. Prevent data from being captured via screenshots / screen-sharing I. Hide or redact data from being viewed on sites
Threat Protection	A. Anti-Phishing Protection B. Advanced Malware scanning	A. Protect users from visiting suspicious websites B. Protect users from suspicious content being downloaded
Access Control	A. Protect Workspace Apps B. Protect GCP Apps C. Protect on-prem Apps D. Protect third-party SAML/OIDC applications	A. Apply Context Aware Access policies to control access to your Workspace applications and Admin console B. Control and monitor access to applications hosted in GCP C. Control and monitor access to applications hosted on-prem D. Control and monitor access to third-party SaaS applications
Investigation	A. Chrome event logs B. Evidence Locker	A. Investigate Chrome events within the Admin Console B. Maintain encrypted copies of files from policy violations for analysis by your security team
Third-party Integrations	A. Integrate with third-party IdPs B. Connectors	A. Utilize CEP telemetry within supported third-party IdPs with Device Trust Connectors B. Send Chrome event logs to security tools (SIEM/SOAR/XDR)

Getting Access

Setup Access for Chrome Enterprise Premium

Prerequisite: Getting Console Access for Your Chrome Enterprise Premium Trial

Once you have your use cases defined, this section will explain how to get the necessary Google Admin Console and Google Cloud Console access *before* you activate your trial. Following these steps ensures you are ready to start as soon as the trial begins.

Scenario 1: Your Organization Already Uses Google Services

Follow these steps if your company uses Google Workspace or Google Cloud.

- 1 **Confirm Existing Access:** You already have the required consoles if your organization uses:
 - **Google Workspace** (for Gmail, Drive, Docs), or manages services like **Chrome OS devices**, **Google Identity**, or **Chrome Enterprise Core**.
 - **Google Cloud** for any production services or projects.
- 2 **Contact Your Administrator:** You will likely need to contact your Google Workspace Super Admin or Google Cloud admin for help. Share this guide with them for instructions on how to enable the trial and create a delegated custom admin role for you.
- 3 **A Note on Permissions for Your Administrator:** Please reassure your admin about the separation of permissions. The custom role created in the Google Admin Console is specifically for managing Chrome browser policies. Rights granted for this role **will not** provide access to the Google Cloud Console, and your organization's resources running in Google Cloud will remain completely untouched.
 - **Advanced Use Case Note:** If Chrome Enterprise Premium needs to be configured to protect services within Google Cloud (for example, through [Google's Secure Gateway](#)), additional rights will be needed, but those are out of scope of this guide.

Scenario 2: Your Organization is New to Google Services

If your organization uses neither Google Workspace nor Google Cloud services, you must create a new account.

- 1 **Understand the Process:** Creating a Google Admin Console is easy and will automatically set up your Google Cloud Console for enabling the trial of Chrome Enterprise Premium at the same time. You'll use a single login for both.
 - Note that the creation of these consoles requires the acceptance of Google's EULA.
- 2 **Sign Up for an Account:**
 - **Visit the sign-up page here:** [Google Chrome Enterprise Sign-Up](#)
 - Provide your business email and follow the on-screen instructions.

Prepare your Test Environment

Prepare for your trial

Get Ready for Your Chrome Enterprise Premium Trial

To get the most out of your 60-day evaluation, use the step-by-step checklist below to prepare your environment *before* activating the trial. This will ensure you can test advanced features from day one without wasting valuable time on basic setup.

Pre-Trial Setup Checklist:

- ☐ [Enable Cloud Identity & Chrome Enterprise Core](#)
 - **Why this is important:** These no additional cost subscriptions create the foundational user and browser management framework required for the premium features to function.
- ☐ [Create a Chrome Enterprise Management Role](#)
 - **Why this is important:** This empowers your evaluation team with the correct permissions from the start, allowing them to immediately access and test the features relevant to their roles without delay.
- ☐ [Create a Organizational Unit Structure](#)
 - **Why this is important:** This is crucial for simulating real-world policy enforcement and testing the difference between device-based and user-based controls.
- ☐ [Enroll Test Browsers and Create Test Users](#)
 - **Why this is important:** A browser must be managed to receive policies. Enrolling your test devices and creating test user accounts ensures they are ready to demonstrate the powerful security and management capabilities you want to evaluate on both managed and unmanaged machines.
- ☐ [Enable Chrome Enterprise Premium Connector Settings](#)
 - **Why this is important:** This turns on the solution's advanced security features for your specific test group and is required for Chrome Enterprise Premium to work.
- ☐ [Deploy Required Browser Extensions](#)
 - **Why this is important:** This extension collects crucial device health and security posture data. Deploying it beforehand enables you to test powerful context-aware and zero-trust access policies from the very start of your trial.
- ☐ [\(Optional\) Set up Device Trust Connector](#)
 - **Why this is important:** If you use a provider like Okta, Ping, or Cisco Duo, this step integrates Chrome's security signals directly into your existing identity and access policies, allowing you to test a seamless, enhanced security posture.
- ☐ [Start a Trial of Chrome Enterprise Premium](#)
 - **You're all set!** With your environment prepared, you can now begin your 60-day trial with confidence, ready to explore all the advanced features immediately.

Enable Cloud Identity & Chrome Enterprise Core

How to Enable your No-Cost Subscriptions

Enable Foundational Subscriptions (Super Admin Required)

This foundational process for user and browser management must be completed by a **Super Administrator**. You will add two services through the Google Admin Console's billing section. This process is at no cost and requires no payment information.

1 Sign In

- Go to admin.google.com and sign in with your Super Administrator account.

2 Go to the Subscriptions Catalog

- From the main menu, navigate to **Billing > Subscriptions**.
- Click the **Buy or upgrade** button.

3 Add Cloud Identity Free

1. In the catalog, select **Cloud Identity** under the Categories section.
2. Under Cloud Identity Free, click **Get Started** and follow the prompts to "check out."
3. Confirm the plan. The total will be \$0.00.
 - **Purpose:** This provides the ability to issue Google identity accounts to manage test users who may not have a paid Google Workspace license, which is essential for applying user-based policies.

4 Add Chrome Enterprise Core

1. Return to the **Buy or upgrade** page.
2. Search for and select **Chrome Enterprise Core**.
3. Click **Get Started** and complete the same free "checkout" process.
 - **Purpose:** This enables centralized cloud management to enroll browsers, enforce policies at the device level, and get visibility into your browser fleet.

5 Verify Your Subscriptions

- Navigate back to **Billing > Subscriptions**.
- Confirm that both **Cloud Identity Free** and **Chrome Enterprise Core** are listed as active subscriptions.

You have successfully enabled the foundational subscriptions and are ready for the next step.

Create a Chrome Enterprise Management Role

Set up admin role in the Google Admin Console

Next, a Super Admin must create a custom role in the Google Admin Console for the Chrome Enterprise Premium trial. Note that permissions in the Google Admin Console are completely separate from the Google Cloud Console; this role will not grant any access to your cloud resources.

Can't find a privilege? On the "Select privileges" page, check both the Admin console privileges and Admin API privileges sections. Duplicates are being consolidated, so a privilege like "Org Units > Read" may be in the API section but functions identically. Here are the steps to create the custom role:

- 1 Go to Account > Admin Roles
- 2 Click the Create new role button and give it a name like "Chrome Enterprise Premium Admin" and click the continue button.
- 3 Select the following Admin console privileges:

Google Admin Console Privileges

Organizational Units Check the box for "Read" (Create, Update, Delete is optional but helpful for testing purposes)

Users Check the box for "Read" (Create, Update, Delete is optional but helpful for testing purposes)

Groups Check the box for "Read" (Create, Update, Delete is optional but helpful for testing purposes)

Security Center Check the box for "Activity Rules" and "This user has full administrative rights for Security Center"

Data Security Check the box for "Rule Management" and "Access Level Management"

Chrome Management Check the box for "Settings"

Chrome DLP Check the box for "Manage Chrome DLP application insights settings", "View and manage Chrome DLP application OCR setting", and "View Chrome DLP application insights settings"

Mobile Device Management Check the box for "Managed Devices and Settings"

Chrome Enterprise Security Services Check the box for "Chrome Enterprise Security Services Settings"

DLP Check the box for "Manage DLP rule" and "View DLP rule"

Alert Center Check the box for "Full access"

Reports Check the box

Google Admin API Privileges

Groups Check the box for "Read"

Organizational Units Check the box for "Read"

- 4 Once selected, click the continue button.
- 5 Click the Create Role button.
- 6 Select the custom role that you created in the previous step and click on the assign role button and assign it to your selected administrators.

Create a Organizational Unit Structure

Separate Devices & User Accounts for Specific Use Cases

To effectively test different security scenarios, you will create a parent Organizational Unit (OU) to contain two child OUs. This structure is crucial for simulating policy enforcement on both corporate and personal devices and makes it easy to manage your entire trial. Note that the admin console also supports Groups, so you can also consider that as an alternative method as well to OUs. Here is [a link for more information about applying policies to Groups](#).

This setup allows you to test three levels of policy application:

- **Parent OU:** Allows you to apply common, baseline policies to both child OUs at the same time, simplifying management.
- **Managed Devices OU:** For testing device-level policies on trusted, corporate-owned browsers.
- **Managed Users OU:** For simulating a Bring-Your-Own-Device (BYOD) scenario by testing user-level policies that follow an account onto any machine.

Steps to Create the OUs:

- 1 Navigate to Organizational Units**
 - Sign in to the Google Admin Console at `admin.google.com`.
 - From the menu, go to **Directory > Organizational units**.
- 2 Create the Parent OU**
 - Select your top level OU and click the **plus** button to create a new OU.
 - **Name:** `CEP Trial`
 - **(Optional) Description:** `Parent OU for Chrome Enterprise Premium trial.`
 - Click **Create**.
- 3 Create the Child OUs**
 - Hover over the `CEP Trial` OU you just created and click the **+** symbol that appears.
 - **Create the Devices OU:**
 - **Name:** `CEP Trial - Managed Devices`
 - **(Optional) Description:** `For corporate-issued devices in the CEP trial.`
 - Ensure the Parent is `CEP Trial`.
 - Click **Create**.
 - **Create the Users OU:**
 - Hover over the `CEP Trial` OU again and click the **+** symbol.
 - **Name:** `CEP Trial - Managed Users`
 - **(Optional) Description:** `For test user accounts created with Cloud Identity.`
 - Ensure the Parent is `CEP Trial`.
 - Click **Create**.

You now have a dedicated structure for applying policies. Moving forward, place all enrolled browsers into the `CEP Trial - Managed Devices` OU and all test user accounts into the `CEP Trial - Managed Users` OU.

Enroll Test Browsers and Create Test Users

Enroll Devices & User Accounts for Specific Use Cases

With your organizational units now in place, the next step is to populate them with the test users and devices you will use for your evaluation of Chrome Enterprise Premium.

Create a Test User Account

- 1 **Navigate to Users:** In the Admin Console, go to **Directory > Users**.
- 2 **Add New User:** Click **Add new user**. For easy identification, name it something like **First Name:** cep, **Last Name:** test.
- 3 **Assign to Correct OU:** Under Manage user's password, **Organizational unit** and profile photo click the dropdown and select the **CEP Trial - Managed Users** OU. This is a critical step.
- 4 **Finalize:** Click **Add New User** and copy the password on the next page.

Enroll a Test Browser (Windows)

- 1 **Navigate and Select the Devices OU:**
 - In the Admin Console, go to **Chrome browser > Managed browsers**.
 - Under the "Managed Browsers" pane select the **CEP Trial - Managed Devices** OU. This ensures browsers are assigned correctly.
- 2 **Generate Enrollment File:**
 - With the correct OU selected, click the **Enroll button**.
 - Under the Downloads section Click **.reg file**. Save the file.
- 3 **Apply on Test Device:**
 - Transfer the downloaded **.reg** file to your test computer.
 - Right-click the **.reg** file and select **Run as administrator**.
 - Accept the security prompts to modify the registry.
- 4 **Verify Enrollment:**
 - Close and **re-open the Chrome browser** on the test machine. It will enroll automatically.
 - You can confirm enrollment in the Admin Console under **Managed browsers** (inside the correct OU) or by typing **chrome://policy** into the browser's address bar on the test device.
 - Alternatively, you can also enroll other OS's (Like Mac OS) for device level browser management via these steps for [Enrolling cloud-managed Chrome browsers](#).

Enable Chrome Enterprise Premium Connector Settings

Chrome Enterprise Connectors and Safe Browsing

To turn on security features, enable the connector and reporting settings on your parent CEP Trial OU; these settings will be inherited by the nested OUs. **Education Customers:** You must also turn on [Chrome Enterprise Security Services](#) (found under [Apps > Additional Google Services](#)), which is required for policies to function.

Configure Chrome Browser Settings

1. In the Admin console, navigate to **Chrome browser > Settings**.
2. On the left, select your parent test OU, **CEP Trial**.

Browser Reporting

- **Managed browser cloud reporting:** Set to [Enable managed browser cloud reporting](#).
- **Event reporting:** Set to [Enable events reporting](#).
- **Managed profile reporting:** Set to [Enable managed profile reporting for managed users](#).
- **Managed browser reporting upload frequency:** Set to 3 hours.
- **Device token management:** Set to [Delete token](#) (Recommended).

Content Connector & URL Check Policies

1. In the settings search bar, filter for **Category contains: "connector"**.
2. Set the primary dropdown to **Chrome Enterprise Premium** for the following policies:
 - Upload Content analysis
 - Download Content analysis
 - Bulk text content analysis (copy/paste)
 - Print content analysis
 - Real-time URL check
 - File transfer content analysis (for ChromeOS)
3. Under **Additional settings** for each, ensure:
 - **Delay until analysis complete:** Check the button
 - **Block on failure:** (Recommended) to enabling this.
 - **Check for sensitive data & malware:** Set to **On**.
 - **Block password protected files and files larger than 50 MB:** Configure as needed.
 - **User justification to bypass warning:** Configure as needed. Recommended to leave disabled for malware.
 - **Minimum character count** (for Bulk text): Set to 1.

Safe Browsing Settings

1. In the settings search bar, filter for **Category: "safe browsing"**.
2. Set the following policies:
 - **Safe Browsing protection level:** [Enhanced mode](#).
 - **Bypass Safe Browsing warnings:** [Do not allow users to bypass](#).
 - **Download deep scanning:** [Enabled](#).
 - **Download restrictions:** [Block malicious downloads](#).

Enable Advanced Data protection Features

1. In the Admin console, navigate to **Security > Access and data control > Data protection**.
2. Under the **Data protection settings** card turn **On** the following features:
 - **Optical Character Recognition (OCR):** Enables scanning for sensitive content within images.
 - **Sensitive content storage:** Stores a copy of sensitive content in log files (and in Evidence locker if configured) that triggers a DLP rule for investigation.

Deploy Required Browser Extensions

Collect device attributes for Context-Aware Access / DLP

Endpoint Verification and the Secure Enterprise Browser are crucial components that gather device data and enable advanced security policies. The following steps will install both extensions.

Important: The following steps should be completed for your parent test OU, **CEP Trial**. Policies will be inherited by the nested OUs containing your test devices and users.

Step 1 Turn on the Endpoint Verification Service

To collect information from devices, the Endpoint Verification service must be active. While this is typically on by default, it's best to confirm.

1. From the Admin console Home page, go to **Devices**.
2. In the navigation menu, click **Mobile & endpoints > Settings > Universal**.
3. Under the **Data Access Card >** Verify that **Endpoint Verification is turned on**.

Step 2 Deploy Required Browser Extensions

This procedure will automatically install both required browser extensions for all users and devices within your specified test OU.

1. **Navigate to Apps & Extensions:**
 - In the Admin console, go to **Devices > Chrome > Apps & extensions > Users & browsers**.
 - Ensure you have selected your parent test OU, **CEP Trial**, on the left.
2. **Add Endpoint Verification Extension by ID:**
 - Click the yellow + icon, select **Add by Chrome app or extension ID**.
 - Enter the ID for Endpoint Verification: **callobklhcbilhphinckomhkgigmfocg**
 - Click **Save**.
 - In the pane that opens, set the **Installation policy** to **Force install + pin to browser toolbar**.
 - Click **Save**. *Do not navigate away from the page.*
3. **Add Secure Enterprise Browser Extension by ID:**
 - Click the yellow + icon again, select **Add by Chrome app or extension ID**.
 - Enter the ID for Secure Enterprise Browser: **ekajlcmdfcigmdbphhifahdfjbkciflj**
 - Click **Save**.
 - In the pane that opens, set the **Installation policy** to **Force install**.
 - Click **Save**.
4. Optionally you can deploy the Native Helper App on your managed devices. For detailed instructions, please refer to the official documentation: [Deploy the Endpoint Verification helper app](#)

(Optional) Set up Device Trust Connector

Link your existing IDP to receive Device Trust Signals from Chrome

This optional section covers setting up a Chrome Enterprise device trust connector.

Objective: To send device-based signals from Chrome to your Identity Provider (IdP) and build them into your authentication flow. This will allow your web applications to verify that users are coming from a managed browser or managed profile in Chrome browser, effectively blocking access from unmanaged browsers and proving the value of context-aware security.

Step 1 Create the Device Trust Connector in Google Admin

1. Sign in to the [Google Admin console](#).
2. Navigate to **Menu > Devices > Chrome > Connectors**.
3. Click **+ New provider configuration**.
4. Find and select your Identity Provider (IdP), then click **Set up**.
5. Enter the required configuration details provided by your IdP.
6. **(Optional for Chrome Browser)** Choose where to apply this configuration:
 - o Managed Browsers Only
 - o Managed Profiles Only
 - o Both Managed Browser and Profiles(Note: This does not apply to ChromeOS, where it is always active).
7. Click **Add configuration**.

Step 2 Apply the Connector to Your Test OU

1. On the **Connectors** page, select your test OU (e.g., **CEP Trial**).
2. Find the **Device trust connectors** setting.
3. From the dropdown menu, select the IdP configuration you just created.
4. Click **Save**.

Next Steps: Build and Test Your Access Policy

With the connector enabled, Chrome now sends device signals to your IdP. The final step is to use these signals to build a context-aware access policy within your IdP's admin console. As an example you could block all browser except Chrome with a managed user or device from accessing your CRM tool by adding device trust signals into a existing authentication flow.

The process for this is specific to each provider.

- [View Specific Setup Guides & Verification Steps for Your IdP](#)

Start a Trial of Chrome Enterprise Premium

Enable the trial in the Google Cloud Console

Follow these steps to activate your 60-day Chrome Enterprise Premium trial:

- 1 **Access the Google Cloud Console:** Navigate to the [Google Cloud Console](#) and sign in with the admin account created in your Google Admin console.
 - Optional but recommended: Create a dedicated project for your CEP trial.
- 2 **Configure Admin Roles:**
 1. First select your Organization (required) at the top right corner and then go to Main Menu > IAM & Admin > IAM.
 2. Locate the admin account you used to sign into the GCP console and click the pencil icon to edit the principal.
 3. In the pop up window that appears, click "Add another role" and search for "Cloud BeyondCorp Subscription Admin", then select it.
 4. Click "Add another role" again, search for "Viewer", select it, and then click "Save".
 5. Note: Additional privileges for Access Context Manager, Compute Engine, and Load Balancing may be necessary to set up policies and create application tunnels.

Please allow *up to 5 minutes* for the roles to populate before going to the next step.

- 3 **Enable the Trial:**
 1. Search for "Chrome Enterprise Premium".
 2. Click the "Sign up" button, then click "Start Free Trial" to enable the trial.
 3. Select the project you wish to apply the trial to.
 4. Your 60-day trial is now enabled. Please allow approximately 5 minutes for it to complete.

- 4 **Assign Licenses:**

A Chrome Enterprise Premium license is required for policies to take effect.

1. Navigate to Billing > Subscriptions.
2. Select Chrome Enterprise Premium.
3. Click the number hyperlink under the Licenses assigned column.
4. Search for your test device or user to confirm the license is applied.
5. Tip: You can also configure automatic license assignment for specific Organizational Units (OUs) or your entire enterprise.

Use cases for Chrome Enterprise Premium

Many of the test use cases for Chrome Enterprise Premium use a similar workflow. We see various scenarios for users on managed or unmanaged devices, so certain Chrome settings might differ for each organization. The following use cases provide a framework of general settings that can be applied for tests that are outlined in the [sample success criteria in this guide](#)

Managed Browser / Profile

Enroll the Chrome Browser and enforce user policies

We covered this in a high level during the setup steps but here are links for additional information and documentation on managing browsers within Chrome Enterprise Core and the other features of managing Chrome browser from the Google Admin console:

- [Chrome Enterprise Core - Setup Guide](#) walkthrough of enterprise Chrome management, enrollment of initial browsers, enable browser/profile reporting, policy precedence, and API support
- [Understand user affiliation](#) for signed-in users that belong to another company domain

Managed and Unmanaged Devices

- [What's the difference between a managed profile and a managed browser?](#)
- [Enroll Browsers via MDM](#) various guides on how to enroll Chrome in your enterprise via MDM
- [Turn on Endpoint Verification](#) required on test profiles in order to gather device attributes
- [Device attributes collected by Endpoint Verification](#) what attributes can be used for device posturing
- [Turn on managed profile reporting](#) view user and device details on actively signed-in users

Reporting and Auditing

- [Reports and data](#) view various reports, configure exports, and other third-party integrations

Password reuse

- [Control password reuse](#) prevent users from using passwords on suspicious sites

Extension Control

- [Apps and extensions](#) methods for auto-installing, permission control, requesting extensions, etc.

Use cases for Chrome Enterprise Premium

Data Protection

Enforce data protection policies through DLP controls

Securely manage access to critical applications and prevent unauthorized data exfiltration of confidential information, even on unmanaged devices. Get started by setting up rules to protect your most sensitive assets.

Before you begin, ensure you have performed the following steps

- [Manage the Chrome Enterprise Data Loss Prevention connectors](#) verify connector status, integrate with third-party DLP vendors (if necessary)

Upload / Download Restrictions, Print Control, Web/URL Filtering, and OCR analysis

- [Use Chrome Enterprise Premium to integrate DLP with Chrome](#) how to setup data protection rules, setup activity alerts, how to enable OCR, and provide DLP / URL filtering rule examples

Copy/Paste Control

- [Data Controls](#) content sources / destinations you wish to protect from unauthorized sharing

Watermarking, Screenshot/screen-share protection, and Data Masking

- [Display watermark on certain webpages](#) to deter misuse on specific URLs
- [Use screenshot / screen-share protection](#) to prevent against potential unauthorized sharing.
- [Perform data masking](#) to protect sensitive information displayed on sites.

Threat Protection

Defend against phishing and malware attacks

CEP provides comprehensive malware protection for your users through real-time URL checks, static and dynamic analysis, and advanced sandboxing. Please refer to the following links to learn more:

- [How Chrome Safe Browsing keeps browsing data private](#) to protect you from things like malicious actors, malware, and phishing attacks
- [Safe Browsing protection levels](#) learn about our enhanced protection mode to warn users about risky sites, dangerous downloads, and untrusted extensions.
- [Protect your data with site isolation](#) separate websites into individual processes in order to prevent data theft
- [Safe Browsing Testing Links](#) resource customers can use to test various threat scenarios

Use cases for Chrome Enterprise Premium

Access Control

Chrome Enterprise Premium (CEP) provides agentless, browser-based security for your modern workforce. Enforce secure access to critical applications on any device and prevent unauthorized data use. This guide covers connecting your apps and creating granular security policies.

Connecting Your Applications

Use Chrome Enterprise Premium's Secure Gateway to route traffic to your web applications without a traditional VPN, reducing latency while enforcing consistent policies.

- **SaaS Applications:** Control access by adding Secure Gateway IP addresses to your app's allowlist for straightforward security checks.
 - [Guide: Secure access to SaaS applications](#)
- **Private Web Applications:** Enforce a zero-trust framework to shield internal apps from public exposure with granular controls.
 - [Guide: Secure access to private web applications](#)

Chrome Enterprise Premium also protects your wider application ecosystem:

- [Secure Google Workspace apps](#)
- [Secure Google Cloud \(GCP\) web applications](#)
- [Secure non-Google Cloud apps using the app connector](#)
- [Configure SAML SSO for Chrome apps](#)

Creating Advanced Context-Aware Access Policies

After connecting your apps, create powerful access policies based on user, device, location, and more.

- **Integrate Security Partner Signals:** Enhance policies by using device posture data from tools like CrowdStrike and Microsoft Intune.
 - [Guide: Set up client-side partner integrations](#)
- **Build Custom Policies:** Use templates for common scenarios like device compliance or time-based access.
 - [See policy examples](#)
- **Combine with DLP:** Customize Data Loss Prevention (DLP) rules based on device security posture for highly specific controls.
 - [Learn how to combine DLP and CAA](#)

Use cases for Chrome Enterprise Premium

Investigation

Gain deep visibility with security events

Visibility of unsafe user activities is one of the most critical aspects of security programs. Chrome Enterprise Premium's Threat and Data Protection captures detailed log events for unsafe user activity so that administrators can monitor, review, and analyze user activities and behaviors, and then mitigate any risks in their organization. Please refer to the following links for more information on viewing and auditing this information.

- [Chrome log events](#) understanding and auditing the different security events
- [Chrome Reporting Connectors](#) to send Security events to your SIEM tool
- [Security Dashboard](#) overview of different security reports (up to 180 days)
- [Security Investigation Tool](#) to identify, triage, and take action on security and privacy issues
- [Evidence Locker](#) to inspect actual files flagged as malware or violating Data Protection rules

Third-Party Integrations

Integrate Chrome with your IDP and various applications

Use Chrome device trust connectors to share context-aware signals from managed Chrome browsers devices with third-party Identity Providers (IdPs). As well as integrate Google into your various corporate apps so users can sign in securely using familiar credentials.

- [Manage Chrome Enterprise device trust connectors](#) for IDPs and third-party integrations (SIEM/XDR)
- [Integrate 3rd-party and custom apps](#) integrate Workspace with other IDPs
- [Deploy private web apps](#) assign apps hosted in GCP, other clouds, or on-premise data centers for users

Troubleshooting Issues

Troubleshooting Chrome Enterprise Premium

This section provides a logical workflow to diagnose and resolve common issues with the initial setup of Chrome Enterprise Premium.

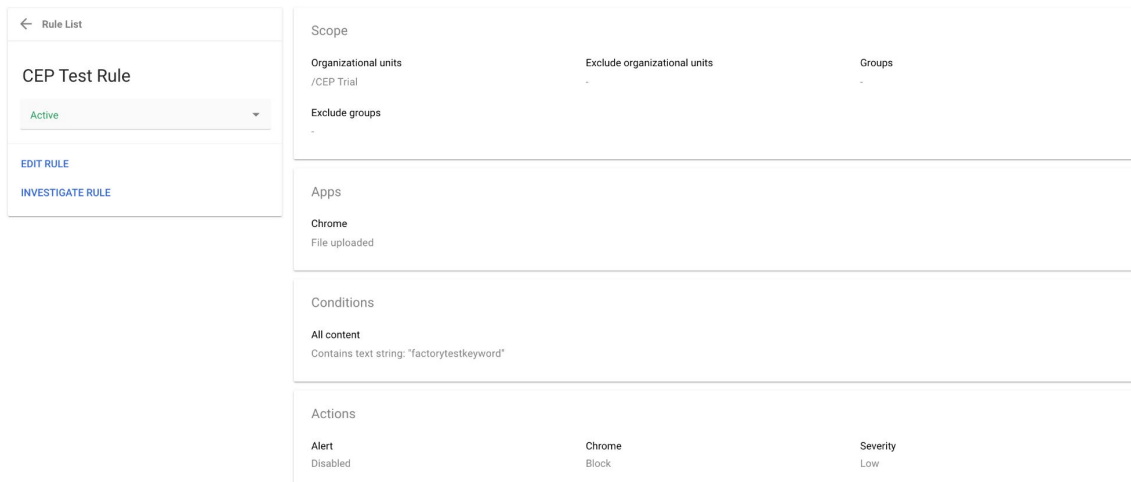
Step 1: The Foundational Check ("Is it plugged in?")

Before investigating a complex rule, confirm the core service is working with a simple baseline test.

1. In the Admin Console go to **Security > Access and data control>Data protection>Manage rules> Add Rule> New Rule**
2. Give it a name like “CEP Test Rule” and select your CEP Test OU under the Scope section.
3. Under the Apps setting select File uploaded under the Chrome section.
4. Click add condition, set it to **All content contains text string** and enter a unique keyword like `factorytestkeyword`
5. Under the actions setting set the action to **Block**. You can add a optional custom message if you wish. Click continue and create on the next screen.

After it is complete, click on the rule and it should look something like this:

Security > Data protection > Rules > CEP Test Rule



The screenshot displays the configuration page for a rule named "CEP Test Rule". The interface is divided into several sections:

- Rule List:** Shows the rule name "CEP Test Rule" and its status "Active". Below this are links for "EDIT RULE" and "INVESTIGATE RULE".
- Scope:** Includes fields for "Organizational units" (set to "/CEP Trial"), "Exclude organizational units" (empty), "Groups" (empty), and "Exclude groups" (empty).
- Apps:** Shows "Chrome" selected, with "File uploaded" as the specific action.
- Conditions:** Shows "All content" selected, with the condition "Contains text string: 'factorytestkeyword'".
- Actions:** Shows "Alert" selected, with "Disabled" as the action type. The "Severity" is set to "Low".

6. **Create a Test File:** On your local machine, create a plain text file (e.g., `dlp_test.txt`) containing only your keyword: `factorytestkeyword`
7. **Test the Rule:** Using a test user or enrolled browser, attempt to upload the file to a site like Google Drive.
 - **If the upload is BLOCKED:** The core system is working. The issue lies with your specific, more complex rule. Try simplifying it to determine the issue.
 - **If the upload SUCCEEDS:** The problem is foundational. Confirm the steps in the previous section to check system settings in the next section.



Troubleshooting Issues

Troubleshooting Chrome Enterprise Premium: Continued



















Step 2: Common Issues (Ruling Out the Simple Stuff)

If your test DLP rule didn't work, verify these common configuration errors in the Google Admin Console.

- **Check the License:** Is an active **Chrome Enterprise Premium license** assigned to the test user or device? Find this under **Billing > Subscriptions**.

Subscriptions		Add or upgrade a subscription	
Name	↑	Status	Licenses
	Chrome Enterprise Core	Active	All licenses
	Chrome Enterprise Premium	Active	40 available, 10 assigned

- **Check Connector Settings:** For DLP to function, security connectors must be set to "Chrome Enterprise Premium."
 - Under additional settings if **Delay file upload** is set to **Allow** immediate action events will only be logged, not blocked.
 - Verify Safe Browsing Mode:** The core threat protection engine requires **Enhanced Safe Browsing** to be enabled.
 - Verify that the user/device belongs to the OU where the connectors are provisioned and where the DLP rule is targeted.**
 - Check out the [Enable Chrome Enterprise Premium Connector Settings section](#) of this guide for all of the specific configuration steps.

Chrome Enterprise connectors			
Setting	Configuration	Inheritance	Supported on
Upload content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Download content analysis	Chrome Enterprise Premium	Locally applied	   iOS
File transfer content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Bulk text content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Print content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Real time URL check	Chrome Enterprise Premium	Locally applied	   iOS

Troubleshooting Issues

Troubleshooting Chrome Enterprise Premium: Continued

Step 3: Diagnostic Tools (Checking the System Logs)

Chrome provides built-in tools to see exactly what the browser is doing. Use these pages to get detailed diagnostic information directly from your test machine. The right pane is going to have the most detailed information.

- **DLP & Malware Events:** `chrome://safe-browsing/#tab-deep-scan`
 - Open this tab *before* you test. It provides a real-time log of security scans. Look for a "result" entry with `triggered_rules` to see which rule fired and what action was taken. If no event appears, the browser isn't evaluating the action.

```
[10/14/2025, 2:44:45 PM]
{
  "request_token": "35D9CE08556EC4C05A5025A542E8A75830E497DD23A7305
5D6B360431F14F49043A97A5072B67B2890E5B2C04F1ADF8D6C8185B8AE3ED1
BEDD4891187DA1CAEF866EEED19D1B2CD57513DC7193E4060D1A030CB5CE9F2
9EBB19FEA0CF74E94EC54BD48E2641E03E253E0CFE1C227D47BC9B1B0FCC7D6
1AFD1BD11BE52C11DA3B",
  "results": [ {
    "status": "SUCCESS",
    "tag": "dlp",
    "triggered_rules": [ {
      "action": "REPORT_ONLY",
      "rule_id": "685305242",
      "rule_name": "[D&R] Evidence Locker file uploads to non-corp domains"
    } ]
  } ]
}
```

- **URL Category Lookup:** `chrome://safe-browsing/#tab-urt-lookup`
 - Open this tab *before* you test, then browse to the site that you are looking to find the category for to see exactly how Google categorizes a specific website. This is essential for troubleshooting URL-based rules, as you must use the precise category name shown here (e.g., `/Internet & Technology/Computer Security`).

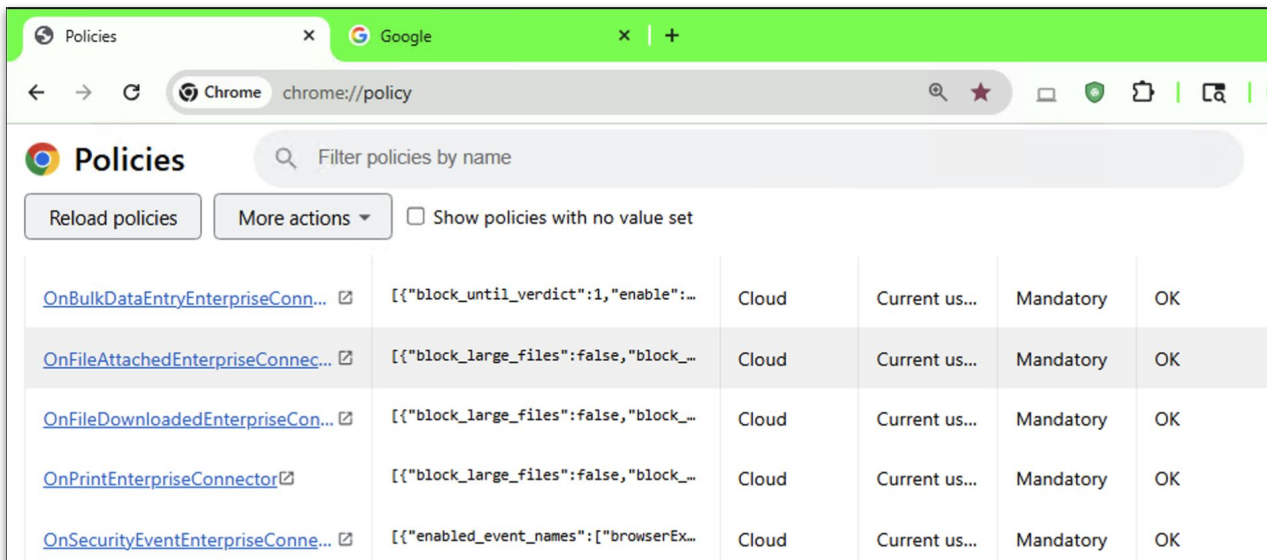
```
{
  "threat_info": [ {
    "cache_duration_sec": "90",
    "cache_expression_match_type": "EXACT_MATCH",
    "cache_expression_using_match_type": "cloud.google.com/free",
    "verdict_type": "SAFE"
  } ],
  "url_categories": [ "/Internet & Technology/Cloud Storage", "/Internet & Technology",
"/Internet & Technology/Enterprise Technology" ]
}
```

Troubleshooting Issues

Troubleshooting Chrome Enterprise Premium: Continued

Step 3: Diagnostic Tools (Checking the System Logs Continued)

- **Applied Policies:** `chrome://policy`
 - This is the definitive source for which policies are active on the browser. Click **Reload policies** to force an update. Look for key connector policies (e.g., `OnFileAttachedEnterpriseConnector`) to ensure they are active.
 - This page is also crucial for identifying policy conflicts and verifying that the machine or user account is enrolled in your domain.
 - If you made a recent change click on “Reload policies” to ensure the Chrome policy is updated.
 - Note: It can take ~ 5+ mins for DLP rules to apply to your machines
 - This image shows a healthy policy with all of the needed based policies configured as [detailed earlier in this guide](#):



OnBulkDataEntryEnterpriseConn...	[{"block_until_verdict":1,"enable":...	Cloud	Current us...	Mandatory	OK
OnFileAttachedEnterpriseConnec...	[{"block_large_files":false,"block_...	Cloud	Current us...	Mandatory	OK
OnFileDownloadedEnterpriseCon...	[{"block_large_files":false,"block_...	Cloud	Current us...	Mandatory	OK
OnPrintEnterpriseConnector	[{"block_large_files":false,"block_...	Cloud	Current us...	Mandatory	OK
OnSecurityEventEnterpriseConne...	[{"enabled_event_names":["browserEx...	Cloud	Current us...	Mandatory	OK

- **Device Signal Issues (CAA):** Endpoint Verification Debug Log
 - Verify that the [endpoint verification and secure enterprise browser extensions](#) are installed under `chrome://extensions` and are enabled.
 - For Context-Aware Access issues, right-click the **Endpoint Verification extension icon** > **Options** > **Show Log**. Look for sync messages and errors, like a failure to connect to the "Native Helper," which is required for advanced device signals.

FAQ

Do I need Google Workspace for user based protections?

Not necessarily. You can use [Google Cloud Identity free](#) for managed user accounts and/or [sync your current IDP with Google](#) to provide user based protections.

Does this support other browsers?

Chrome Enterprise Premium only operates within the Google Chrome Browser, however there are features in the solution that can prevent your sensitive data from being accessed by other browsers.

Does this solution support incognito windows?

You can leverage the [Data Controls](#) policy to restrict what data can be shared between apps, browsers, and profiles (including incognito). Additionally, you can restrict whether users can browse in incognito mode as well.

How is data collected by Chrome?

Data that is collected varies by the configuration set by the administrator.

- If the device is enrolled in Chrome Management with reporting turned on, then you can refer to [this document for more information about what data is collected](#).
- If Chrome security event reporting is turned on, then you can refer to [this document for more information about what data is collected](#).
- Additional information on [Chrome log events and attributes can be found via this link](#)

Additional Resources

Chrome Enterprise Premium



[Chrome Enterprise Premium Overview](#)



[Purchasing Chrome Enterprise Premium](#)

Chrome Enterprise Core



[Chrome Enterprise Core Overview](#)



[Setting up Chrome Management](#)



[Chrome Management Deployment Guide](#)

Chrome Browser Integrations



[Chrome Browser Reporting Connectors](#)



[Chrome Browser Device Trust Connectors](#)