chrome enterprise

Chrome Enterprise Premium Trial Guide

April 2025

chrome enterprise

Table of Contents

chrome enterprise

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:

- 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

chrome enterprise

Define the scope of your test

Define your success criteria

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.

chrome enterprise

Define the scope of your test

Sample success criteria

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	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
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	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)

chrome enterprise

Prepare your Test Environment

Set up access and prepare for your trial

In order to make the most of your 60-day trial of Chrome Enterprise Premium, it is recommended to have access and devices setup prior to turning on the trial. Here are the steps in order with links on how to accomplish them so you are ready to get started!

1. Get access to a Google Admin Console or use your existing one.
2. Gain access to a Google Cloud Console or use your existing one.
    a. Note if you are setting up a Google Admin console for the first time, you also get a Google Cloud Console created at the same time.
    b. You can use the same login for both.
3. The *Superadmin* will need to enable the tenant for both Cloud Identity free and Chrome Enterprise Core billing subscriptions (if you don't already have them).
4. The *Superadmin* can now enable the CEP Trial.
5. Setup roles in each console for your CEP admins.
    a. Setting up roles in the Google Admin Console
    b. Setting up roles in the Google Cloud Console
6. Admins can enable the connector settings for CEP for their test OU's or Groups.
7. Enroll browsers in Chrome Enterprise Core on your managed (test) devices.
8. Deploy endpoint verification extension to your managed (test) devices or user accounts.
9. (Optional) Set up Device Trust Connector for additional functionality if you use Ping, Okta or Cisco Duo as your IDP.

Once these steps are complete then you will have your environment ready to go.

chrome enterprise

Start a Trial of Chrome Enterprise Premium

Enable the trial in the Google Cloud Console

1. Go to the Google Cloud Console
2. Do a search for Chrome Enterprise Premium
3. Click the Sign up button and then click the “Start Free Trial” to enable the trial.
4. Select the project that you want to trial to applied to.
5. Your 60 day trial is now enabled, please wait ~ 5 minutes for it to complete.
6. You can now click on the “Learn how to assign users to Chrome Enterprise Premium licenses” link to apply your trial to user accounts or devices within the Google Admin console.
7. You must license the admin user and any devices/user accounts before proceeding to the next step. This can be done under > Billing > License settings > Assign Licenses. You can also auto assign licenses via these steps.

Enable Security Insights and begin testing

Now that you have your environment setup, accounts created and devices enrolled, you are ready to start testing! Please refer back to the test plan that you created in the previous step and use these sections to test out the protections of Chrome Enterprise Premium

- Analyze high risk insider and data exfiltration activities
- No impact to the end user as it is reporting only
- Build reports to guide you towards what steps to take to further secure your data in the browser.

To enable Security Insights, follow these steps:

1. Head to admin.google.com and click the Home page tab on the left
2. In the top right corner, you will see an option to “Enable monitoring for insider risk and data loss”

   Make sure that you have super admin privileges as it is needed to turn this on.
3. Click on the Enable button on the bottom of the pop up screen.

At this point you will most likely want to let Chrome collect details on user actions and activity for the next week or two for a better view of your data usage and threat landscape.

Once this has completed, you will be provided with multiple reports that can be drilled into for better understanding and visibility.

Through these reports you determine what areas of concern might need additional attention and layered security controls. These can be found under the Security Center dashboards on the left side of the Admin Console.

chrome enterprise

Set up your Google Admin Console Account

Set up admin role in the Google Admin Console

Google Admin Console needed Privileges

A custom role in the Google Admin Console will be need to be created. You will need to have sufficient privileges to create custom roles.

1. Go to Account > Admin Roles
2. Click the Create new role button and give it a name like “Chrome Enterprise Premium Admin” and hit 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)
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
Organizational Units Check the box for “Read”

4. Once selected hit the continue button.
5. Hit 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.

chrome enterprise

Set up your Google Cloud Admin Account

Set up admin role in the Google Cloud Console

Google Cloud Console needed Privileges

A custom role in the Google Admin Console will be need to be created to enable the trial of Chrome Enterprise Premium. You will need to have sufficient privileges to create custom roles.

1. Login as your admin account created in the Google admin console and Go to Main > IAM & Admin > Roles"
2. Click the Create new role button to create an org-level role and give it a name like "Chrome Enterprise Premium Admin". Make sure that you are creating this with your organization selected.
3. Select the following privileges:

Google Cloud Console (Set at Org level)
GCP Viewer Role (needed to see resources and projects)
Access Context Manager Admin "accesscontextmanager.gcpUserAccessBindings.list"
Cloud BeyondCorp Subscription Admin "beyondcorp.subscriptions.list"
Select all the permissions related to "accesscontextmanager"

Additional permissions may be required for access context manager, compute engine, and load balancing to setup policies and create necessary app tunnels.

You will also need to select the permissions in multiple pages

4. Click on "CREATE" to finish
5. Go to "Main > IAM & Admin > IAM", and click on "ADD" to add an admin user

   Make sure you are performing this action at the ORG level
6. Choose your admin user in "New members" area
7. Select "Custom > Chrome Enterprise Premium Admin" as the Role
8. Click on "SAVE" to finish
9. On this same screen, change to the project that you would like to use for testing
10. Note the "Chrome Enterprise Premium Demo" project next to "Google Cloud Platform"
11. Click on "ADD" to add permissions for the admin user
12. Select your admin user in the "new members" area
13. Choose "Basic > Owner" as the role
14. Click on "SAVE" to finish

chrome enterprise

Enable Connector Settings

Chrome Enterprise Connectors and Safe Browsing

This section provides some tips on how to setup the threat and data protection features of CEP.

1. Ensure that the managed device or user account that you are testing has a Chrome Enterprise Premium license applied.
    - You can do via Billing > Subscriptions > Select “Chrome Enterprise Premium" and click on the blue hyperlink that says “# assigned” under the Licenses column and search for the device or user account that you are troubleshooting
2. Verify that Chrome Enterprise Premium settings are enabled via “Security Insights” and correctly applied to the Organizational Unit or Group you are testing.
    - You can do this via Chrome browser > Settings > filter for Category contains “connector” and verify that the following is set:
        - “Allow enterprise connectors” is set to “Allow users to enable Enterprise Connectors”
    - Verify that the following settings are set to “Chrome Enterprise Premium” in the drop down:
        - Upload Content analysis (“allow” for audit / delay = for “warn” or “block”)
        - Download Content analysis (same as above)
        - Bulk text content analysis (same as above, set minimum character count to 1)
        - Print content analysis (same as above)
        - Real time URL check (set to CEP)
    - **Note**: While you review the mode settings for each feature, under “Additional settings” review the modes to your preferences.
        - On by default, except for the following URL patterns (bypass or not)
        - User justification to bypass warnings (force user to provide justification for action)
3. Verify that Safe Browsing settings are enabled and correctly applied to the Organizational Unit or Group you are testing.
    - You can do this via Chrome browser > Settings > filter for Category contains “safe browsing” and verify that the following is set:
        - Safe Browsing protection set to “enhanced mode”
        - Disable bypassing Safe Browsing warnings “Do not allow”
        - Allow download deep scanning for Safe Browsing-enabled users “Enabled”
        - Download restrictions “Block malicious downloads”

chrome 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

Once you have reviewed the findings from the Chrome Security Insights report from the previous steps, then you can start reporting on enrolled browsers and signed-in profiles for investigation. Please refer to the following links on getting started:

Before you begin, ensure you are signed up for Chrome Enterprise Core and perform the following steps

- 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.

chrome enterprise

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 and Screenshot protection

- Data Controls content sources / destinations you wish to protect from unauthorized sharing

Watermarking

- Display watermark on certain webpages to deter unauthorized sharing for specific URLs

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

chrome enterprise

Use cases for Chrome Enterprise Premium

Access Control

Connect your SaaS, private web, and on-premise applications

Supporting remote or contracted users can be challenging when you don't have the ability to push traditional agents to unmanaged machines. By using CEP, you can enforce access to critical apps, with an agentless solution to prevent unauthorized usage of sensitive company information. Please refer to the following links on getting started:

- Protect your business apps with Context-Aware access how to secure your Workspace apps
- Securing Google Cloud web applications how to setup and protect your GCP resources
- Secure non-Google Cloud apps using the app connector how to setup and use the CEP App Connector to secure a non-Google Cloud app
- Configure SAML single sign-on for Chrome apps follow the relevant SAML vendor's documentation to properly configure federated single sign-on authentication for their services
- Client-side partner integrations setup sharing of third-party client device posture signals (Crowdstrike Falcon ZTA and Microsoft Intune)

Creating advanced Context-Aware Access policies

- Context-Aware Access examples for Advanced mode provides examples of sample conditional access policies you can use as templates (authentication, device, time-based access, etc.)
- Combine DLP rules with Context-Aware access conditions customize your DLP rules based on the security posture of the device used while the user is accessing various web resources

chrome enterprise

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

chrome enterprise

Troubleshooting Issues

Browser-Side Troubleshooting

This section provides some tips on how to troubleshoot the threat and data protection features. Most of the debug screens are in “chrome://safe-browsing”, including

1 chrome://safe-browsing/#tab-rt-lookup

This tab shows all the URL analysis events and what the results are

Below is an example of the RT URL check when you tried to go download a safe CSV file


```
{
  "dm_token": "ABjmT7kMHtEiDhVFYvEAXO_xdM0C-tIZwZTe3-bbdpMuzAvQCN5U2jKULX40pxJ
iqURvuhYXBphcKwgW-AmLyGRsIwexkmyPtCpKyEtjjiLOiBqrb7G7UMl1_JqXshV5DEAYb2_pZFTAI
a2HY5TRrIZfDPqCZYRnbde9ovSX0d5zDWzUczeRtqEnHvxBgq3ptDyensyP4oHatZv3AfhyPvY9I
YDU-2Ay5q2ScaKsbklu6u007vv6HC8=",
  "lookup_type": "NAVIGATION",
  "os": "LINUX",
  "population": {
    "finch_active_groups": [ ],
    "is_history_sync_enabled": true,
    "is_incognito": false,
    "is_under_advanced_protection": false,
    "profile_management_status": "UNAVAILABLE",
    "user_population": "EXTENDED_REPORTING"
  },
  "scoped_oauth_token": "",
  "url": "https://dlptest.com/sample-data.csv",
  "version": 1
}
```

```
{
  "threat_infos": [ {
    "cache_duration_sec": 300.0,
    "cache_expression": "dlptest.com/sample-data.csv",
    "cache_expression_match_type": "EXACT_MATCH",
    "cache_expression_using_match_type": "dlptest.com/sample-data.csv",
    "threat_type": "THREAT_TYPE_UNSPECIFIED",
    "verdict_type": "SAFE"
  } ]
}
```


2 chrome://safe-browsing/#tab-deep-scan

This tab shows all the content analysis events (malware, DLP) and what the results are.

Below is an example of the DLP and malware check for the CSV file

- CSV is not a supported file type for malware check so no rules should be triggered
- It does show, however, the DLP rule getting triggered


```
[5/1/2021, 3:55:22 AM]
{
  "analysis_connector": "FILE_DOWNLOADED",
  "device_token": "ABjmT7kMHtEiDhVFYvEAXO_xdM0C-tIZwZTe3-bbdpMuzAvQCN5U2jKULX40p
xJiqURvuhYXBphcKwgW-AmLyGRsIwexkmyPtCpKyEtjjiLOiBqrb7G7UMl1_JqXshV5DEAYb2_pZFTA
Ia2HY5TRrIZfDPqCZYRnbde9ovSX0d5zDWzUczeRtqEnHvxBgq3ptDyensyP4oHatZv3AfhyPvY9IY
DU-2Ay5q2ScaKsbklu6u007vv6HC8=",
  "fcm_notification_token": "d1Rhf-6b4gU:APA91bHV9udIssAr2Yx2SEJHxmdwSMgEzPYV8EpbaC
JBthYnEpFsujKftcEpZ7dfwb9wH13a2oPMxdynwsJuonrLgrpJNrtIdWCEPLCHmhkItWvve1rJs2RqpC
p2AbsjJ5tnQJEsDkgH",
  "request_data": {
    "digest": "9D3407981112133A7FA74A804A300F93BD5520500AAD06008F1F8D898464132
B",
    "filename": "sample-data (1).csv",
    "url": "https://dlptest.com/sample-data.csv"
  },
  "request_token": "0E74F887F4B7D24C77CB9A197036E4ADC47FCE2EE3B86BB223FC6FCCA
5AE909B55C056FA95A576E52C3D9587AD7A7C34EDD2B14897EDD59D3265EB17310F56BDE
835DC02A991A8F372953517A038CAB4B5F2667F3479919850867E3FC2510719EE4604D5DD
F24D6A606C5821FA5F62F0B9D9F776A15B16C7871579BAEB09F656",
  "tab_url": "https://dlptest.com/sample-data.csv",
  "tags": [ "dlp", "malware" ]
}
```

```
[5/1/2021, 3:55:23 AM]
{
  "results": [ {
    "status": "SUCCESS",
    "tag": "dlp",
    "triggered_rules": [ {
      "action": "WARN",
      "rule_id": "245165307",
      "rule_name": "[jzhen] Test DLP rule"
    } ]
  }, {
    "status": "SUCCESS",
    "tag": "malware",
    "triggered_rules": [ ]
  } ],
  "token": "0E74F887F4B7D24C77CB9A197036E4ADC47FCE2EE3B86BB223FC6FCCA5AE909B
55C056FA95A576E52C3D9587AD7A7C34EDD2B14897EDD59D3265EB17310F56BDE835DC02
A991A8F372953517A038CAB4B5F2667F3479919850867E3FC2510719EE4604D5DDF24D6A6
06C5821FA5F62F0B9D9F776A15B16C7871579BAEB09F656"
}
```

chrome enterprise

Troubleshooting Issues

Browser-Side Troubleshooting

3 **chrome://safe-browsing/#tab-reporting**

This tab shows all of the event logs we send from Chrome to Security Center
Below is an example of the log message that was sent for the DLP trigger


```
{
  "sensitiveDataEvent": {
    "clickedThrough": false,
    "contentSize": 4750,
    "contentType": "text/csv",
    "downloadDigestSha256": "9D3407981112133A7FA74A804A300F93BD5520500AAD06008F1F8D898464132B",
    "eventResult": "EVENT_RESULT_WARNED",
    "fileName": "/usr/local/google/home/jzhen/Downloads/sample-data (1).csv",
    "profileUserName": "jzhen@beyondcorp.joonix.net",
    "trigger": "FILE_DOWNLOAD",
    "triggeredRuleInfo": [ {
      "ruleId": "245165307",
      "ruleName": "[jzhen] Test DLP rule"
    } ],
    "url": "https://dlptest.com/sample-data.csv"
  },
  "time": "2021-05-01T03:55:23.143Z",
  "uploaded_successfully": true
}
```


If you expect certain behavior and are not seeing it, use one of those URLs in a new tab to see whether the logs reflect what you expect to see.

Note: These tabs must be OPEN at the time of the request before the events show up.

To verify that the Chrome policies are configured, in a new Chrome tab of the protected profile window, go to “chrome://policy” and click on “Reload policies” to ensure the Chrome policy is updated

Depending on what you have set, you should see some or all of the following policies applied

OnBulkDataEntryEnterpr…	{ "block_until_verdict": 0, "enable": [{ "tags": ["dlp"], "ur…	Cloud
OnFileAttachedEnterpris…	{ "block_large_files": false, "block_password_protected": false,…	Cloud
OnFileDownloadedEnter…	{ "block_large_files": false, "block_password_protected": false,…	Cloud
OnSecurityEventEnterpri…	{ "service_provider": "google" }	Cloud

chrome enterprise

Troubleshooting Issues

Console-Side Troubleshooting

1. **License Check** (verify status = active, licenses are correctly assigned to correct OUs / Users)

Subscriptions Add or upgrade a subscription

Name	Status	Licenses
Chrome Enterprise Core	Active	All licenses
Chrome Enterprise Premium	Active	40 available, 10 assigned
Cloud Identity Free	Active	5,040 available
Cloud Identity Premium	Active	40 available, 10 assigned
Google Workspace Enterprise Plus	Active	4,990 available, 10 assigned

2. **Chrome Enterprise Premium connector settings** (verify connector settings)

Chrome Enterprise connectors

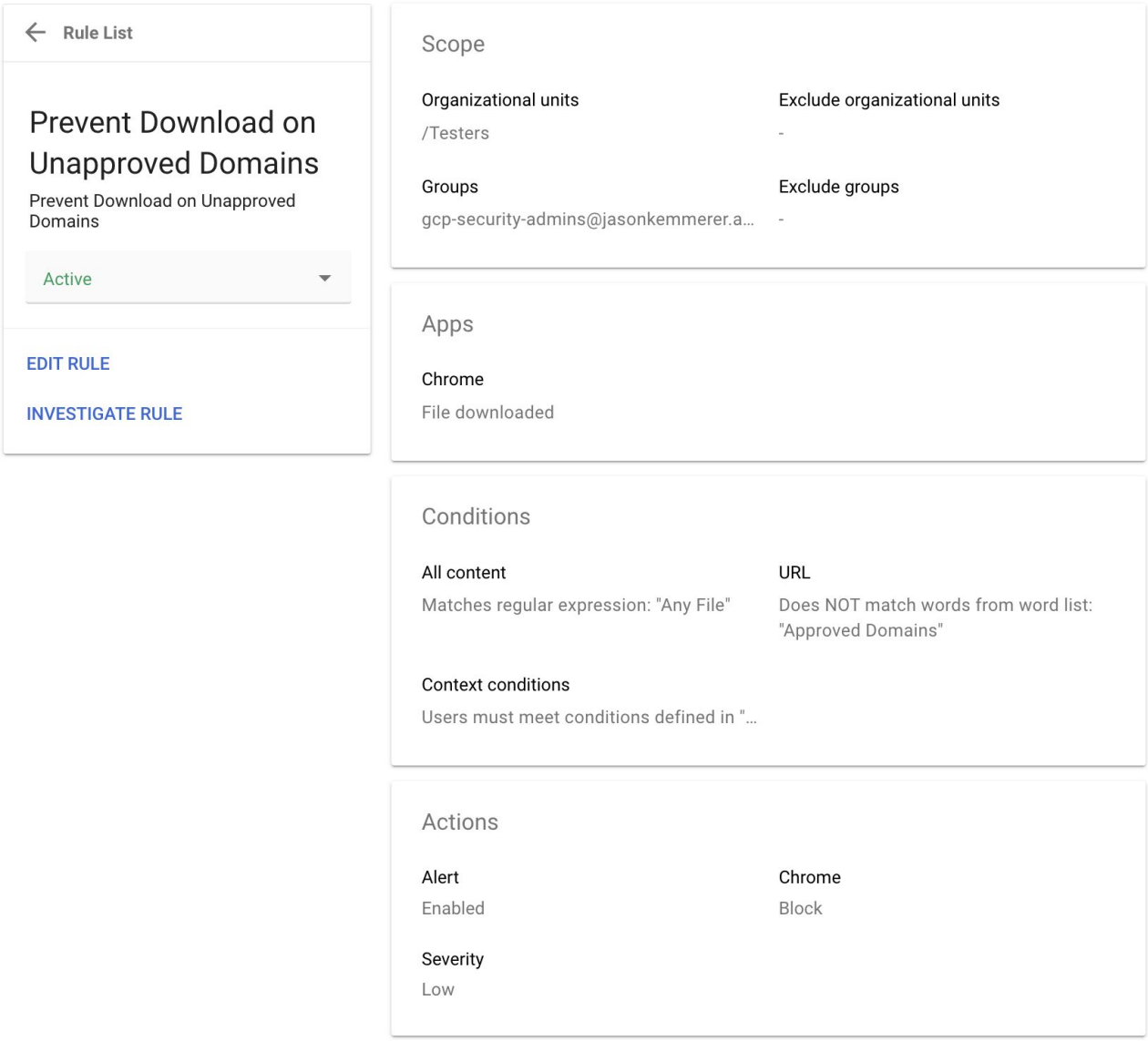
Setting	Configuration	Inheritance	Supported on
Allow enterprise connectors	Allow users to enable Enterprise Connectors	Google default	
Upload content analysis	Edit in legacy view	Locally applied	
Download content analysis	Edit in legacy view	Locally applied	
File transfer content analysis	Edit in legacy view	Google default	
Bulk text content analysis	Edit in legacy view	Locally applied	
Print content analysis	Edit in legacy view	Locally applied	
Real time URL check	Chrome Enterprise Premium	Locally applied	

chrome enterprise

Troubleshooting Issues

Console-Side Troubleshooting

3 **Verify DLP Rule** (ensure the scope, apps, conditions, and actions are correct)



chrome enterprise

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