chrome enterprise

Chrome Enterprise Premium Setup Guide

April 2024

chrome enterprise

Table of Contents

chrome enterprise

Chrome Enterprise Premium Overview

Secure enterprise browsing is the the emerging standard of protecting your corporate data of protecting your corporate data while enabling your users to work securely on the web from anywhere with any device. Chrome Enterprise Premium provides:

- Robust data loss prevention
  - Customizable controls to safeguard sensitive information.
- Proactive threat defense
  - Real-time protection against phishing, malware, and sandboxed threats.
- Granular access management
  - Restrict access to critical applications based on the principle of least privilege.

This guide will provide you with the steps to set up Chrome Enterprise Premium for user or device (or both) 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 user's devices
- A license for Chrome Enterprise Premium
- Access to a Google Admin console
- Access to a Google Cloud Console
- Devices enrolled into Chrome Browser Cloud Management and/or Google Cloud Identity licenses for users to be managed

chrome enterprise

Use cases covered by this guide

Chrome Enterprise Premium provides a variety of different features that address many common use cases for enterprises.

This guide will address the most common and effective controls that you can apply quickly and efficiently:

1. Mitigate insider and data exfiltration risks from corporate, and third party partners.
2. Manage access and security for applications and resources for managed and unmanaged devices
3. Simplify and reduce your VDI footprint providing secure access to critical applications.

chrome enterprise

User vs device management

Picking the right solution for your use case

Chrome Enterprise Premium provides support for both user based and device based enforcement of policies. **Note: You can setup both user and device based management if you wish. For more information about user vs device management , please take a look at [this help center article.]**

Here is an overview what each offering supports:

		User based management	Device based management
Supports unmanaged machines	Apply policies and security browser enforcements on non-company issued devices	✓	
Mandatory Device level policy enforcement	Apply policies and security browser enforcements to all user profiles without requiring users to sign into Chrome		✓
Sync Chrome data across multiple machines	Chrome data (e.g. history, bookmarks etc.) can be moved from machine to machine if the user signs in.	✓	
Chrome integrations	Chrome Connectors Integrations into Identity providers (e.g. Okta, Ping etc), send security event reports to SIEM tools (e.g. Chronicle, Splunk etc)	✓	✓
Chrome Security Insights	Chrome Security Insights reporting	✓	✓
Advanced Chrome Security	Malware Deep Scanning	✓	✓
	URL Categorization & Filtering	✓	✓
	Real-time phishing detections	✓	✓
	Data Loss Prevention (including Context Aware Access and DLP features)	✓	✓
	Evidence Locker (saving content when a data protection rule is triggered for investigations)	✓	✓
	Context Aware Access for SaaS Apps and Private Web Apps via Chrome	✓	✓

chrome enterprise

Get started

Access options for Chrome Enterprise Premium

In order to setup user or device based management of Chrome browser, you need access to a Google Admin console and a Google Cloud Console. Note that there are two options to get access to the admin console:

Option 1: Don't have Google Admin console?

- Follow this link to setup your account and follow the process to verify your domain.
- A Google Cloud Console will also be available for access using this process. Users logging into the Cloud Console will be prompted to accept GCP terms of service upon login.
- The console itself is provided at no additional cost.

Option 2: Already have a Google Admin Console?

- If the console is already set up, Chrome Browser Cloud Management is already present, you just need to activate it. Check out these steps to add it to your subscriptions at no additional cost.
- A Google Cloud Console is also already set up

If it is possible to use your company's existing Google Admin console, that is the best option. You will need to contact your super admin to give you the proper rights to manage Chrome policies and set Chrome Enterprise Premium security controls. See the following page for more details.

Get started

Setting up admin roles In the Google Admin console

Google Admin console needed privileges

A custom role in the Google Admin console will be need to be created. A super admin account is required 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	
Organizational Units	Check the box for Read, Create, Update (Delete is optional but recommended)
Chrome Management	Check the Settings box to provide all rights to Chrome management.
Security Center	Check the box for This user has full administrative rights for Security Center
Data Security	Check the box for Access Level Management, Rule Management
Alert Center	Check the box for Full access
Chrome DLP	Check the box for Manage Chrome DLP application insights settings, View Chrome DLP application insights settings
DLP	Check the box
Chrome Enterprise Premium	Check the box
Reports	Check the box

4. Once the above are 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 the “assign role” button and assign it to your selected administrators.

chrome enterprise

Get started

Setting up admin roles In the Google Cloud Console

Google Cloud Console needed privileges

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

1. Go to “Main > IAM & Admin > Roles”, and click on “CREATE ROLE” to create an org-level role and give it a name like “Chrome Enterprise Premium Admin”.

   The following rights are needed in order to enable the license for Chrome Enterprise Premium and additional configurations:

Google Cloud Console (Set at Org level)
GCP Viewer Role (Org and Project is needed to see resources and projects)
Cloud BeyondCorp Admin Role (Org Level and Project Level)
Cloud BeyondCorp Subscription Admin Role (Org Level)

   You will also need to select the permissions in multiple pages:

2. Click on “CREATE” to finish

3. 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
4. Choose your admin user in “New members” area
5. Select “Custom > Chrome Enterprise Premium Admin” as the Role
6. Click on “SAVE” to finish
7. On this same screen, change to the project that you would like to use for testing
8. Click on “ADD” to add permissions for the admin user
9. Select your admin user in the “new members” area
10. Choose “Basic > Owner” as the role
11. Click on “SAVE” to finish

chrome enterprise

Setup managed users and / or devices

Managing Chrome Policies in the Admin console

Chrome Enterprise Premium advanced threat and data controls are enabled with policies set in the Google Admin console. You will need to either create managed user accounts or enroll devices into the console to enforce these policies. Chrome cloud policies can be applied at signed-in user or machine level and can provide protections and visibility in different ways. It is recommended to use device based management for corporate managed devices and user based management for your extended workforce. See the table below for the difference between the two management methods:

Cloud policy scope	User (profile)	Machine (device)
Typical use-case	• Unmanaged device / contractor provided devices • Corp users on BYOD	Corp owned device
Policy enforcement	Upon user sign-in to Chrome	No sign-in (or identity) required
Policy granularity per device	Enforced at individual user level	Enforced across all Chrome profiles
License requirements	Google Identity or Google Workspace User licenses	None
Admin configuration	Configure Chrome browser policies	• Generate and deploy enrollment token via OS level policy (i.e. GPO) to devices • Configure Chrome browser policies
Security event reporting granularity	Signed-in user activity reported	Device level reporting across all profiles, user information is not reported
Chrome Browser reporting (extension, version)	Presently not available at the per profile level	Available across the device reporting on all profiles.

You will need to enroll browsers in Chrome Browser Cloud Management and/or create managed Google user accounts before proceeding to the next steps. Below are the details on setting either scenario (device or user):

- **User based management:** Chrome cloud user-profile configuration help center article
- **Device Based management:** Chrome cloud machine (device) help center article or Setup Guide in Admin console

NOTES

- If you are presently managing Chrome policies at the OS level (i.e. GPO for Windows) Chrome cloud policies can coexist together, you do not need to change existing Chrome policy processes to enable Chrome Enterprise Premium policies in the Admin console.
- When there is a policy conflict, Chrome adheres to a default policy precedence, there are policies to help merge policies or to override the default precedence.

chrome enterprise

Start a trial of Chrome Enterprise Premium

Enabling a trial in your Google Cloud Console

1. Go to the Google Cloud Console.
2. Do a search for “Chrome Enterprise Premium”.
3. Click “Sign up” and then click “Start Free Trial” to enable the trial.
4. Select the project to which you want the trial applied.
5. Your 30 day trial is now enabled, please wait ~ 5 minutes for it to complete.
6. You can use this link on “Learn how to assign users to Chrome Enterprise Premium licenses” for instructions on how 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 Chrome Security Insights

After enabling the trial and setting up your admin accounts, you can turn on "Chrome Security Insights” to do a security review of your environment. Through this no-cost review you can:

- Analyze high risk insider and data exfiltration activities
- No disruption is caused to your end users
- Build reports to guide you towards what steps to take to further secure your data in the browser

To set this up, 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 “Monitor data leaks and insider risks”
    - 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. More information about this feature is available via this help center article.

Once the collection process is completed, you will be provided with multiple reports that can be drilled into for better understanding and visibility. Note that if you have already enabled Chrome Enterprise Connectors, the Chrome Security Insights will not enable and your configuration will stay in its existing state.

These reports will help you to 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

Use cases for Chrome Enterprise Premium

Many of the use cases for Chrome Enterprise Premium use a similar setup. Depending upon whether you are supporting managed or unmanaged devices/users, the settings might differ.

The following use cases provide a framework of general settings that can be applied using Chrome Enterprise Premium.

Use case 1. Mitigate insider and data exfiltration risks

Setting up DLP rules in the Admin console

Once you have reviewed the findings from the Chrome Security Insights report from the previous steps, you can start setting up rules to protect your most sensitive assets. Please refer to the following links on getting started:

- Enable Chrome Enterprise Premium settings in the Google Admin console
- Turn on Data Loss Prevention rules in the Google Admin console
- Managing Endpoint verification for managed devices
- Protecting data with Context-Aware Access
- Combine Data Loss Prevention rules with Context-Aware access conditions

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.

- Understanding and auditing the different security events in the Google Admin console
- Use Chrome's Reporting Connector to send Security events to your SIEM tool
- Using the Security Dashboard in the Google Admin console
- Using the security investigation tool to inspect and remindate security events

chrome enterprise

Use cases for Chrome Enterprise Premium

Use case 2. Manage access and security for employees using unmanaged devices

Setting up Context-Aware Access

Supporting remote or contracted users can be challenging when you don't have the ability to push traditional agents to unmanaged machines. By using Chrome and Chrome Enterprise Premium, you can enforce access to critical apps, with an agentless solution to prevent downloading, saving, pasting, copying or printing of sensitive company information.

Please refer to the following links on getting started:

- Enable Chrome Enterprise Premium settings in the Google Admin console
- Turn on Data Loss Prevention rules in the Google Admin console
- Combine Data Loss Prevention rules with Context-Aware access conditions

Integrate Chrome with your IDP through Device Trust connector

Chrome Enterprise device trust connectors share context-aware signals from managed Chrome browsers and ChromeOS devices with third-party Identity Providers (IdPs). This integration allows device trust signals as inputs in authentication and authorization policies.

- Manage Chrome Enterprise device trust connectors in the Google Admin console

Protecting Private Web Apps through Chrome Enterprise Premium

Private web applications are created for an organization's internal users, such as employees and contractors. These apps can be deployed using Chrome Enterprise Premium in the Google Admin console and provide support for apps hosted in Google Cloud or other clouds and on-prem data centers.

Please refer to the following links on getting started:

- Adding the app to your Workspace Account
- Settings for apps hosted on Google Cloud
- Settings for apps hosted on other cloud providers or on-prem data centers
- Restrict access and authentication

Use cases for Chrome Enterprise Premium

Use case 3. Simplify and reduce your VDI footprint

Setting up Context-Aware Access

Legacy VDI solutions can be costly, complex to set up, and difficult to secure and use. Through Chrome Enterprise Premium you can enable users to securely and directly access private web apps like they would a SaaS application.

Customers are now using technologies like application streaming to provide secure application delivery as a replacement for VDI that can be integrated with Chrome Enterprise Premium security features for a complete secure container solution.

Use case 4. Control access to shadow IT with better visibility

Prevent users from accessing risky web apps and stop data exfiltration

Whether accidental or malicious, user actions can jeopardize corporate data by storing it in less than secure SaaS. By enabling Chrome Enterprise Premium, you can:

- Leverage URL filtering to block risky unsanctioned SaaS applications and prevent users from visiting insecure websites
- Enable data protection rules to block file transfers (download, upload, save, copy, paste, print) on unmanaged devices and warn users on sensitive data transfer on managed devices
- Enable Chrome Device Trust Connectors to provide seamless authentication without the need to modify SAML flows

Please refer to the following links on getting started:

- URL navigation rule examples
- Block Chrome navigation to a custom URL list
- Chrome Device Trust connectors

Troubleshooting data protection features

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

chrome://safe-browsing/#tab-urt-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 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"
  } ]
}
```


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, however, show 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:APA91bHV9udlssAr2Yx2SEJHxmdwSMgEzPYV8EpbaC
JBthYnEpFsujKftcEpZ7dfwb9wH13a2oPMxdynwsJuonrLgrpJNrtIdWCEPLCHmhkltWvve1rJs2RqpC
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"
}
```

Troubleshooting data protection features

Browser-side troubleshooting

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 data protection features

Console-side troubleshooting

This section provides some tips on how to troubleshoot the threat and data protection features in the Google Admin console at admin.google.com

- Ensure that the managed device or user account that you are troubleshooting has a Chrome Enterprise Premium license applied
  - You can do this 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.
- Verify that Chrome Enterprise Premium settings are applied in the “Organizational Unit” that the device or user account is in.
  - You can do this via Chrome browser “Settings>“ filter on “Category Contains” “connector” and verify that the following is set:
    - Allow enterprise connectors is set to “Allow users to enable Enterprise connectors”
  - Depending on what you have configured for the device you may need to verify that the following is set to “Chrome Enterprise Premium” in the drop down:
    - Upload Content analysis
    - Download Content analysis
    - Bulk text content analysis
    - Print content analysis
    - Real time URL check
  - It is also a good idea to review the “mode” setting under “Additional settings” for each feature that you enable as some may be set to “Off by default, except for the following URL patterns”.
- If troubleshooting a specific rule (like a DLP rule looking for sensitive data) verify that it is applied to the “Organizational Unit” that contains the device or user account that you are troubleshooting.
  - You can do this under the “Rules” section, select the rule that you are troubleshooting and check the following:
    - Verify that the rule is active
    - Check under the scope to make sure that it contains the “Organizational Unit” that you are troubleshooting
    - Click “investigate rule” to see if the device or user account that you are troubleshooting shows up under the logs as triggering the rule
  - If the above points are correct, click on “cancel” to exit the rule editor.
- Refer to this guide for troubleshooting access errors in the Google Cloud Console.

chrome enterprise

FAQ

What is Chrome Enterprise Premium and how much does it cost?

Chrome Enterprise Premium brings together the most trusted enterprise browser with Google's advanced security capabilities — building upon the capabilities available in Chrome Enterprise Core and offering additional advanced security capabilities, including: enterprise controls, security insights, context-aware access controls, and threat and data protection.

Chrome Enterprise Premium is licensed per user account. Please contact your sales rep for additional information on pricing. You can learn more about Chrome Enterprise Premium here.

FAQ

Does Chrome Enterprise Premium require Google Workspace?

No, Google Workspace is not required. Chrome Enterprise Premium complements Google Workspace by adding to the additional data protections that are provided to solutions like Drive and Gmail, but it's not required.

What operating systems are supported?

Chrome Enterprise Premium currently supports all desktop platforms including Windows, Mac, Linux and ChromeOS. iOS and Android are both supported for mobile access to web applications when leveraging context aware access policies.

Does Chrome Enterprise Premium support any install of Chrome?

Both user based installs and managed installs of Chrome browser are supported. No special version of Chrome browser is required and no additional agents are needed. So this makes the solution easy to manage and deploy via your current management methods.

What is Chrome Enterprise Core?

Chrome Enterprise Core offers core management capabilities at no additional cost. It gives IT teams the power to centrally manage and secure Chrome across their organization, regardless of device platform. Learn more here.

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 Chrome Enterprise Premium support other browsers?

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

Does Chrome Enterprise Premium support Incognito windows?

The solution does not include support for activity in Incognito windows. For information about how to prevent users from opening new Incognito windows, read about the Incognito mode setting.

What data is collected by Chrome Enterprise Premium?

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

- If the device is enrolled in Chrome Browser Cloud 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

chrome enterprise

Additional Resources

Chrome Enterprise Premium

- Chrome Enterprise Premium Overview

Browser Management

- Chrome Browser Cloud Management Overview
- Setting up Chrome Browser Cloud Management
- Chrome Browser Cloud Management Deployment Guide

Third-Party Integrations

- Chrome Browser Reporting Connectors
- Chrome Browser Device Trust Connectors
- Chrome Browser Data Loss Prevention Connectors