chrome enterprise

cisco

Cisco Secure Access and Chrome Enterprise

Joint Solution Guide



Workforce protection with Cisco Secure Access and Google Chrome Enterprise Premium

This solution guide outlines how Cisco Secure Access integrated with Chrome Enterprise Premium to deliver robust workforce protection along with an intuitive and seamless user experience. This joint solution offers a secure way to access private web apps via the browser using Chrome Enterprise. Together they safeguard against data breaches, phishing attempts, and enforce zero trust access controls. Employees and the extended workforce can work confidently with transparent and easy-to-manage Data Loss Prevention (DLP) and authentication protocols. Together, Cisco Secure Access and Chrome Enterprise Premium protect your data, allowing users to work securely from anywhere on any managed or unmanaged device.

© 2025 Cisco and/or its affiliates. All rights reserved.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

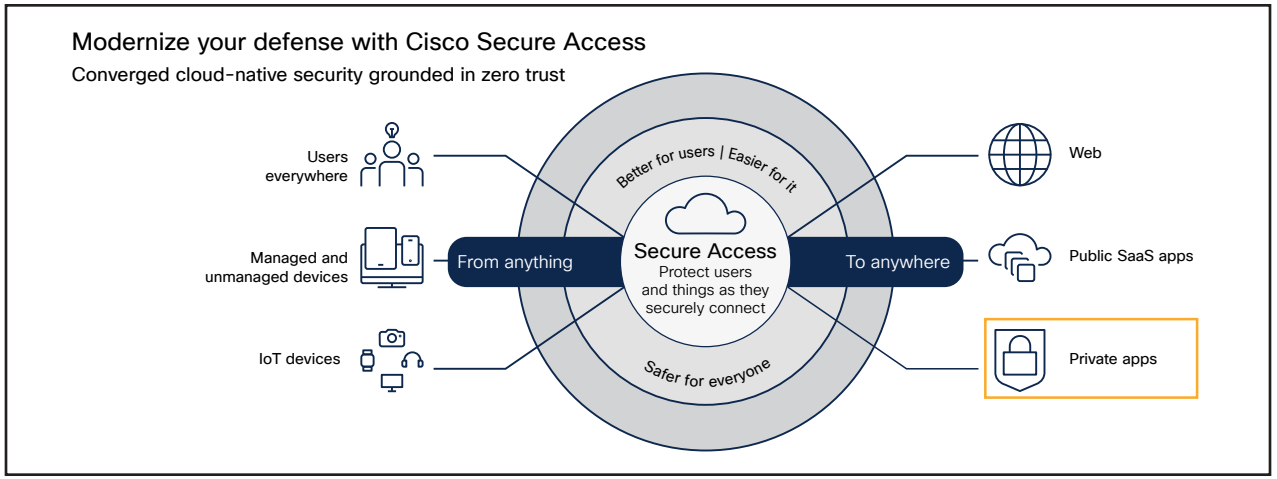
Solution overview

Cisco Secure Access customers with an active Chrome Enterprise Premium license can use this solution guide to set up secure remote access to private web apps with enhanced threat and data protection. The logical mix of local and cloud-based capabilities results in a great end user experience, better performance and reduced risk.

Cisco Secure Access overview

Cisco Secure Access is a cloud-based SSE solution, grounded in zero trust, that provides seamless, transparent, and secure access from anything to anywhere. It includes all of the core SSE components (SWG, CASB, ZTNA, and FWaaS) plus an extended set of capabilities (protections for AI use, multimode DLP, DNS Security, RBI, sandboxing, DEM insights, and AI-powered Talos threat intelligence) in one license and management platform.

By leveraging these capabilities, all under one cloud-delivered platform, organizations can solve a variety of security challenges. Users can now safely and seamlessly access all the resources and apps they need, regardless of protocol, port, or level of customization. Enforce modern cybersecurity to radically reduce risk and delight users and IT staff by addressing today's challenge of safely connecting anything to anywhere.



chrome enterprise

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

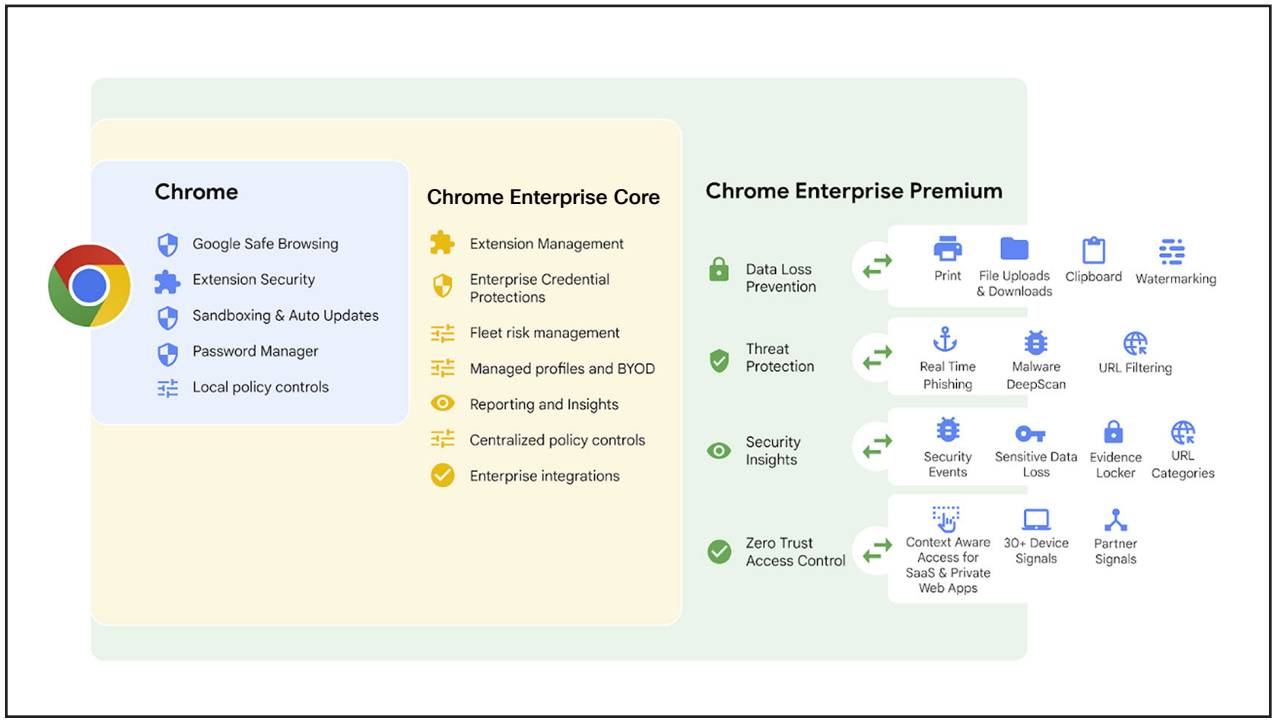
Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Access is built on a backbone of modern cybersecurity technologies, is designed to fundamentally reduce risk, radically simplify IT operational complexity, and minimize tasks required of end-users. For more information see Cisco Secure Access.

Google Chrome Enterprise overview



Chrome Enterprise Premium allows organizations to use the same secure and reliable browser employees love and adds critical controls and protections forIT and security teams. Organizations using Chrome Enterprise Premium benefit from Google's world-class threat intelligence, AI-powered security features and zero trust access via Google's secure global network, ensuring data protection and user safety.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Chrome Enterprise Premium offers additional advanced security capabilities, including:

- Controls to enforce enterprise policies, manage software updates and extensions.
- Security insights and reporting that support event reporting, device reporting, and forensic capabilities for enterprise-wide visibility, and can integrate with other Google and third-party security solutions.
- Context-aware access controls that can be scaled for web applications, help enforce continuous Zero Trust access to SaaS and web-based apps, and can mitigate data exfiltration risks.
- Threat and data protection that delivers content inspection and data loss prevention, anti-malware, and anti-phishing using frontline intelligence and AI, dynamic URL filtering, and site categorization.

For detailed information see Chrome Enterprise Premium.

Combined private application process

The collaboration delivers both improved security and a better user experience on both managed and unmanaged devices. This provides high-performance private application access with robust posture information and data security controls, including a deep set of combined data loss protection capabilities. It is especially helpful for third-party/contractor access and VDI migration.

Through Zero Trust Network Access (ZTNA), Cisco Secure Access uses least privilege principles and contextual insights to deny access by default and allow access to apps as configured for users authenticated to a Chrome Enterprise browser. Chrome Enterprise Premium provides an additional layer of user and data controls to harden private app security.

End-user experience

Paula, a contractor working for ACME, opens her Chrome Browser and signs into a new profile using her enterprise identity. Chrome understands that Paula belongs to ACME, creates a work profile for her enforcing enterprise browser controls and reporting.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Since Paula's administrator has also enabled the Secure Access integration, Chrome shares her device posture signals with Secure Access for access enforcement. Secure Access assesses the device posture signals and assesses the device posture and private access rules before providing access to Paula. Because Secure Access uses the MASQUE (Multiplexed Application Substrate over QUIC Encryption) protocol to proxy web traffic, only the intended traffic dictated by ACME's private access policy is intercepted; everything outside of that specific policy flows directly to the Internet.

Based on the policies ACME has configured, in-browser protections such as watermarks and screenshot protections are enforced on the Jira website. Additionally, any data that Paula uploads or downloads via the Chrome Enterprise browser is scanned for sensitive data or malware. Chrome Enterprise Premium policies make sure no malicious or unvetted extensions can modify the Jira ticketing system. Finally, ACME admins can get detailed security insights about all the activity happening within their managed browser environments.

Admin experience

To get started and access detailed configuration and administration information:

- Cisco Secure Access: Getting Started.
- Chrome Enterprise Premium: Getting started.

Configure Cisco Secure Access

This section assumes that you have a fully configured and deployed Cisco Secure Access organization. For additional instructions on setting up private resources and private resource policies, please see below. Otherwise, proceed to the next section.

- **Configure Private Resources:** Private resources include private subnets and applications deployed and managed by your organization.

For detailed instructions on setting up private resources, see documentation here.

- **Configure Private Access Policies:** Private access policies allow you to define granular user-based access to private resources.

Detailed configuration instructions are available here.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Setting Up Chrome Enterprise Premium Integration with Secure Access

1. Configure Chrome Enterprise Premium integration.

Login to your Cisco Secure Access dashboard (dashboard.sse.cisco.com) and navigate to Admin > Third-party Integrations. Click the Integrate button on the Chrome Enterprise Premium tile.

- Step 1. **Google Admin Console Configuration** – login to your Google Admin Console (admin.google.com) and navigate to Devices > Chrome > Connectors. Click on New Provider Configuration. Scroll to Cisco Device Trust and click Set Up. Provide a meaningful name for Configuration Name. From the Chrome Enterprise Premium integration in the Cisco Secure Access dashboard, copy the service account and URL patterns from their respective fields into the Cisco Device Trust Connector fields. Click Add Configuration.

2. Create a new browser-based endpoint posture profile for Chrome Enterprise Premium.

Login to your Cisco Secure Access dashboard (dashboard.sse.cisco.com) and navigate to Security > Endpoint Posture Profiles. Click Add posture profile and select Browser-based.

- Step 1. Select operating systems required for private app access. Not selecting any operating system will allow any operating system.
- Step 2. Select Chrome Enterprise Premium as the required browser for private app access.
- Step 3. Require firewall if the device should have an active firewall running for private app access.
- Step 4. Require disk encryption if the device should have disk encryption enabled for private app access.

Click Save and Exit.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Configure Chrome Enterprise Premium

- **Start with Chrome Enterprise Core:** Begin your journey to protect Cisco Secure Access users and data with Chrome Enterprise Core – a free tool offering centralized control over Chrome browser policies and security across Windows, Mac, Linux, iOS, and Android. Gain invaluable security insights by identifying outdated browsers, installed extensions, and potential vulnerabilities within your organization. Get started here.
- **Enhanced Protection on Managed Devices:** Simplify management and strengthen protection by enforcing enterprise policies and security settings directly at the browser level on fully managed devices. This eliminates the need for user sign-ins for policy enforcement.
- **Enable Data and Threat Protections with Chrome Enterprise Premium:** Empower yourself with Chrome Enterprise Premium capabilities to protect against data loss and malware threats. Define granular controls within user profiles, enabling sensitive data checks, malware content protection, and customized file analysis with flexible actions for uploads and downloads.
- **Enable Security Insights:** IT teams can leverage Chrome Enterprise's security reporting to gain valuable insights into potential threats Google Workspace users may encounter while browsing. Once security event reporting is enabled, audit logs provide detailed information on malicious site visits, malware-infected file activity, unsafe password practices, and extension installations. Additionally, these security events can be exported into Google Cloud products like Pub/Sub or Chronicle, or leading third-party security solutions such as Splunk, Crowdstrike, and Palo Alto Networks.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Key use cases

The scope of this guide will focus on the use cases related to the combined solution that comprises Google's Chrome Enterprise Premium and Cisco's Secure Access. All other use cases and features of each solution will work as-is without any modification.

Cisco Secure Access: Zero Trust Private Access Use Cases

Provide superior risk mitigation

Least privilege access, unique traffic micro-segmentation to block lateral movement and the obfuscation of app locations to block reconnaissance activities.

Offload overburdened IT

No need to procure, install, maintain hardware and do load balancing.

Deliver a better user and administrator experience

Frictionless access for users. Single agent, console, identity and posture for IT.

Enable more granular control

Fine-tune access controls to safeguard critical resources.

Cisco Secure Access utilizes an innovative zero trust access approach that will:

- Keep multiple, individual user to app sessions from piggybacking onto one tunnel and decreasing the potential of a significant security breach.
- Use a reverse proxy that utilizes next-generation protocols with the ability to support per-connection, per-application, and per-device traffic streams to ensure no direct resource access.
- Ensure complete obfuscation of your internal resources so proper access is granted without sharing resource location or network details.
- Confirm posture and authentication checks take place on a per session basis with credentials specific to a particular user without risk of sharing.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

- Obtain awareness into user activity by fully auditing sessions from the user device to the applications without being hindered by proprietary infrastructure methods.
- Shrink the timescale and minimize risk exposure around Certificate Authorities that issue certs and hardware-bound private keys with multi-year validity.

Chrome Enterprise Premium use cases

- Enhanced Data Loss Prevention (DLP) – Preventing unauthorized data leakage.
- Advanced threat protection and access controls – Preventing use credential leakage as well as robust defense mechanisms against external threats and sophisticated access controls.
- User and entity behavior analytics – Preventing unauthorized credential entry and providing clear visual cues to enhance awareness.
- Advanced Browser Controls – Policy enforcement, compliance, and browser management.
- Enhanced device trust - Simplified endpoint trust with simpler and agent free access policies.

Data loss prevention

Chrome Enterprise Premium, when deployed in conjunction with Cisco Secure Access, provides a powerful solution to mitigate the risk of sensitive Private Web App data leakage due to accidental or malicious insider activity.

Key capabilities

Chrome Enterprise Premium empowers enterprises to implement highly granular controls over data movement within protected browser profiles:

- **Customized data handling rules:** Define precise rules dictating the types of data permitted for upload, download, print, watermarking, URL filtering and copy/paste operations across sites.
- **Real-time DLP enforcement:** Content involved in uploads, downloads, or cross-site pasting actions is automatically analyzed against your configured DLP rules.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

- **Flexible user actions:** Based on the severity of detected violations, the system can issue warnings, or actively block users from completing the intended action.

Steps to set up DLP for Chrome Enterprise Premium

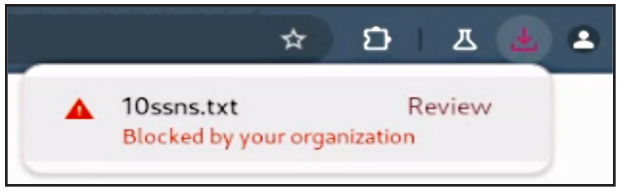
- **Step 1:** Set up Chrome Enterprise connector policies. Go to Set Chrome Enterprise connector policies for Chrome Enterprise Premium in Chrome Enterprise's Help Center for details.
- **Step 2:** Set up data protection rules in Google Workspace Admin console.
- **Step 3.** Set up activity alerts. Go to View alert details (also in Google Workspace Admin Help) for descriptions of alert types.

Local DLP use cases

1. Prevent users from bulk downloading sensitive data from Cisco Secure Access protected enterprise applications

Once Cisco Secure Access is configured for secure user access to your private web applications, you can leverage Chrome Enterprise Premium to tightly control downloads. This includes blocking unauthorized downloads based on:

- **Sensitive content detection:** Block downloads containing pre-configured data patterns like Social Security numbers or credit card numbers.
- **Download behavior:** Prevent downloads exceeding certain size thresholds or downloads from suspicious sources within your private web apps.
- **Monitoring and alerts:** Set up activity alerts to gain visibility into the volume and types of data downloaded from your private web applications.



chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

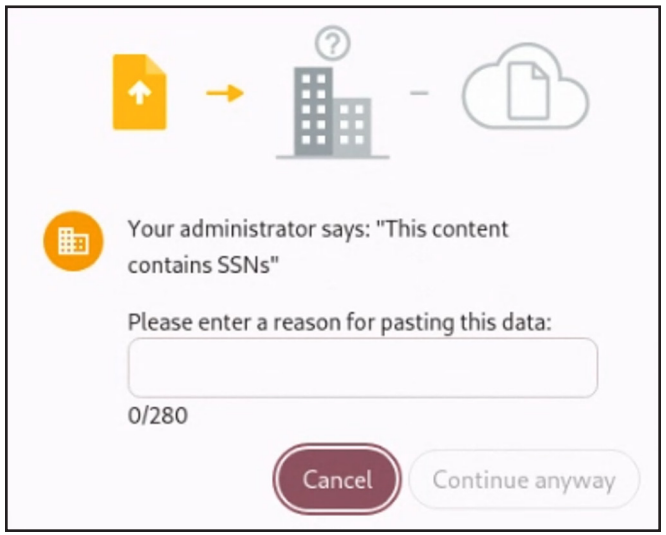
Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

2. Prevent users from copying data from a Cisco Secure Access protected enterprise application and pasting it into unsanctioned websites

Data exfiltration often involves users copying confidential information from enterprise applications and pasting it into unsanctioned websites like Pastebin. To combat this, Chrome Enterprise Premium's paste data protection rules give you granular control:

- **Sensitive content detection:** Block pastes containing pre-configured data patterns like Social Security numbers or credit card numbers.
- **Allowlisting/Blocklisting:** Define specific enterprise applications where pasting sensitive data is either permitted or explicitly prohibited.
- **Flexible actions:** Choose to block, warn, or simply log attempts to paste sensitive data from Cisco Secure Access protected enterprise apps into unsanctioned destinations.



chrome enterprise

cisco

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

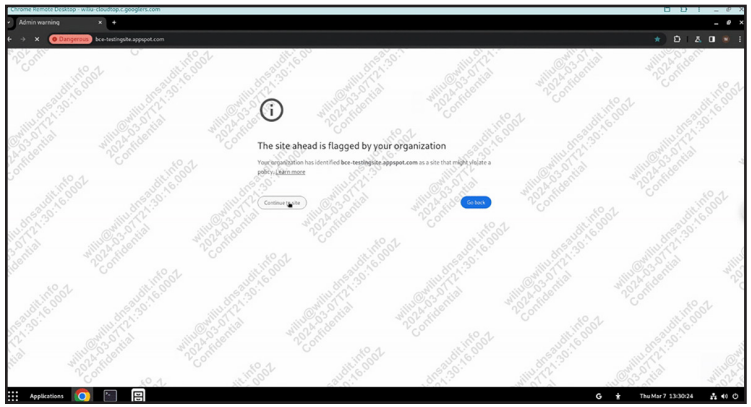
Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

3. Prevent users from printing pages from Cisco Secure Access protected enterprise applications

Data exfiltration can also happen through printing sensitive documents from enterprise applications. Chrome Enterprise's printing data protection rules provide precise control to mitigate this risk:

- **Sensitive content detection:** Block printing of files containing pre-configured data patterns like Social Security numbers or credit card numbers.
- **Flexible actions:** Choose to block, warn, or simply log attempts to print sensitive data.
- **Monitoring and alerts:** Set up activity alerts to gain visibility into the volume and types of data being printed from your private web applications.



4. Add a watermark to Cisco Secure Access protected enterprise applications

Chrome Enterprise Premium allows administrators to add a customizable, translucent watermark to protected private applications. This visual deterrent discourages users from taking screenshots or photographs, a common data exfiltration tactic.

- **Customizable text:** Administrators can customize the text that appears in the watermark which can also include user email address, timestamp etc in order to facilitate investigations.
- **Monitoring and alerts:** Set up activity alerts to gain visibility into the volume and details of which pages are being protected using watermarking.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

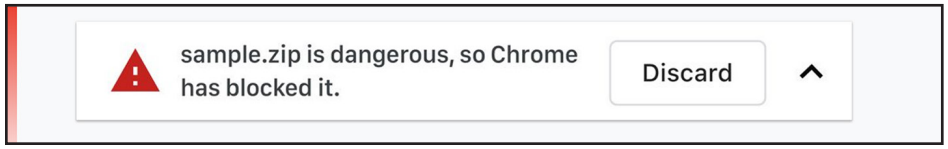
Threat protections

Chrome Enterprise enabled through Chrome Enterprise Premium, safeguards your users against malware and phishing threats during file uploads and downloads. Here's how it works:

1. **Real-Time URL check:** Chrome instantly compares the source website's URL against Google Safe Browsing's vast database of known malicious sites. If deemed unsafe, you can block the action or log the incident.
2. **Metadata analysis:** If the site is safe, Chrome Enterprise Premium examines the file's metadata (hashes, certificates, signatures) using Google Cloud's advanced malware detection.
3. **Optional sandboxing:** For files requiring deeper scrutiny, you can opt for analysis in Google Cloud's secure sandboxes. Files can be delayed pending verification or released immediately with background checks.
4. **Flexible actions:** Administrators can block downloads/uploads based on verification results or choose to log incidents. Detailed monitoring logs provide visibility into threats faced.

Malware protections

When you activate Chrome Enterprise Premium, Google Safe Browsing automatically scans uploads and downloads within Chrome Enterprise browsers, leveraging advanced malware detection technology. If Safe Browsing identifies a malicious file, Chrome will alert the user. Administrators have the flexibility to allow users to bypass these warnings or completely block access to malicious files. Detailed monitoring logs provide insights into malicious activity, including which users encountered warnings, malware signatures, and the associated URLs.



Learn more about how to enable Malware Protections in Chrome Enterprise Premium.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

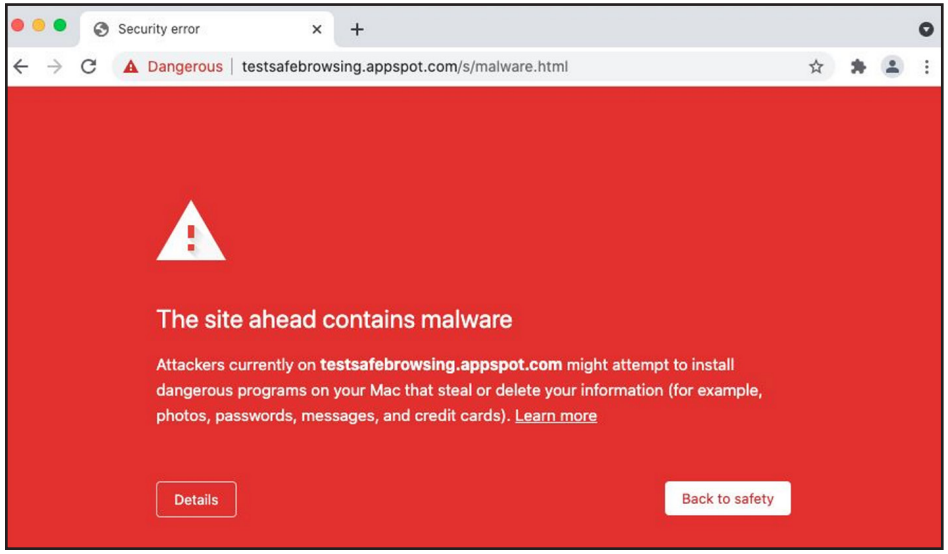
Threat protections

© 2025 Cisco and/or its affiliates. All rights reserved.

Phishing protections

Chrome Enterprise Premium employs real-time URL checks. When users navigate within protected profiles, Chrome instantly compares visited URLs against the Safe Browsing database. This database contains millions of known malicious and unsafe websites. Administrators can choose whether users can bypass these warnings or enforce stricter blocking policies.

This real-time protection helps safeguard your organization from evolving online threats.



Learn more about how to enable Phishing Protections in Chrome Enterprise Premium.

chrome enterprise

CISCO

Contents

Workforce protection with Cisco Secure Access and Chrome Enterprise

Solution overview

Combined private application process

Configure Cisco Secure Access

Configure Chrome Enterprise Premium

Key use cases

Data loss prevention

Threat protections

Sanctioned extension access

Extensions pose a large security risk. Many extensions request powerful permissions that if misused, could lead to security breaches or data loss. However, due to strong end user demand, it's often not possible to fully block the installation of extensions.

- Apps and Extensions usage report**:** Provides visibility into every Chrome extension that is installed across an enterprise's fleet. Admins can force install or block any extension across any segment of their fleet.
- Extensions workflow**:** Admins can decide under which circumstances an extension install needs to be reviewed by IT. A review workflow in the Google Admin console makes it easy for admins to review and approve install requests for specific users requesting an extension, or for their broader fleet.
- Extensions details**:** Admins can see additional details about an extension's permissions, and other relevant metadata. This info is surfaced in the Extensions list and Extensions workflow pages to make it easier for administrators to manage extensions.

Customers who have Cisco Secure Access and Chrome Enterprise Premium deployed can also use enterprise policies in order to prevent extensions from altering Private Web Application pages served via Cisco Secure Access.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C07-4435933-01 04/25