chrome enterprise

CISCO
The bridge to possible

Cisco Secure Access and Chrome Enterprise

Joint Solution Guide

Workforce protection with Cisco Secure Access and Chrome Enterprise

Cisco Secure Access and Chrome Enterprise work together to deliver robust workforce protection. This joint solution offers a secure way to access private web apps using managed Chrome browsers. It safeguards against data breaches, phishing attempts, and enforces 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 and Chrome Enterprise secure your data, allowing users to work securely from anywhere on any managed device.

chrome enterprise

CISCO
The bridge to possible

Contents

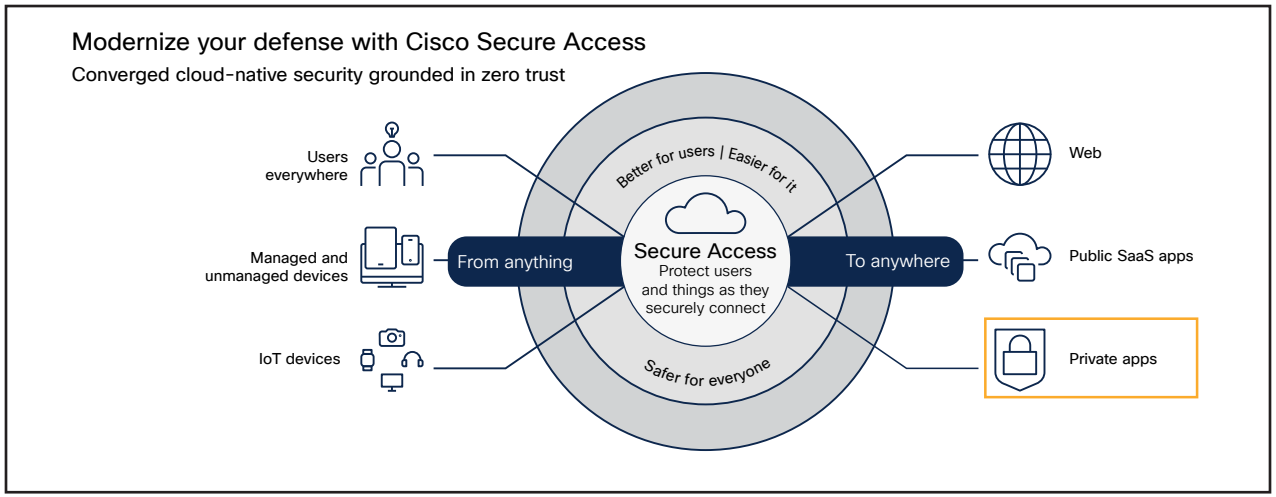
Solution overview

Customers with both Cisco Secure Access and Chrome Enterprise Premium can use this solution guide to configure remote access to private web apps with enhanced threat and data protection capabilities that are a result of this combined approach. 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 converged 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 (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.



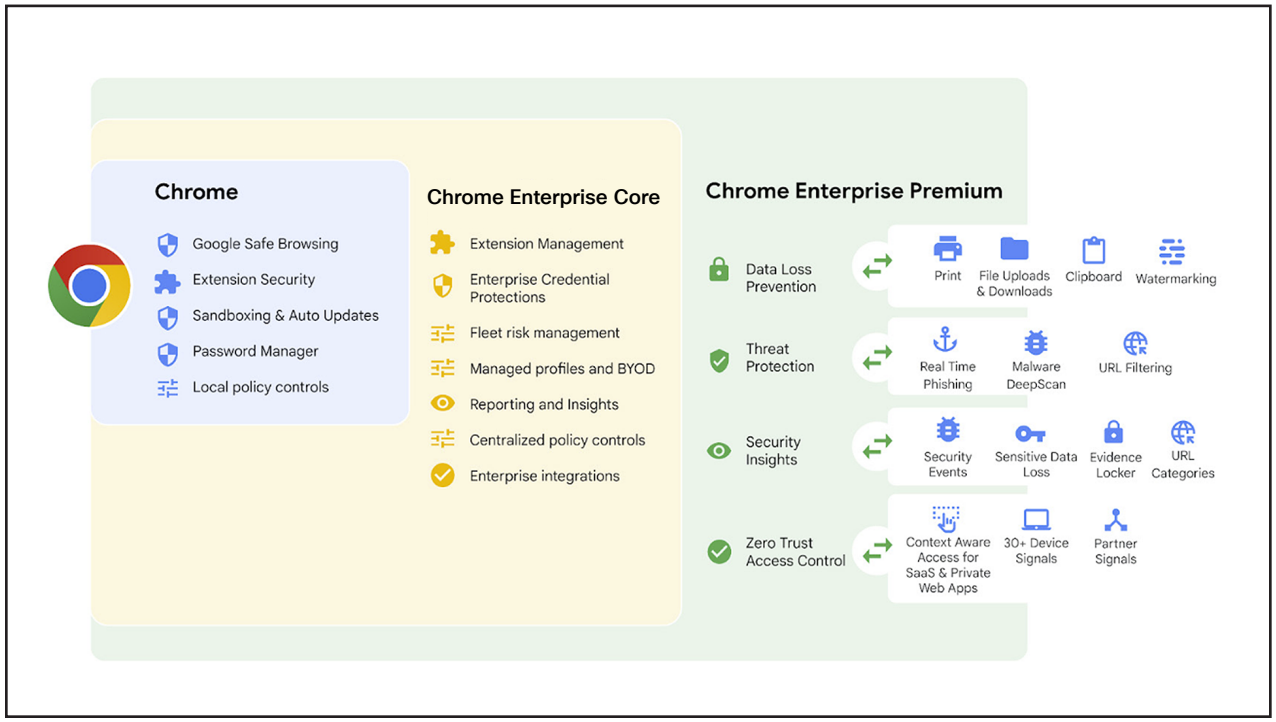
chrome enterprise

CISCO
The bridge to possible

Contents

Secure Access enforces modern cybersecurity, while fundamentally reducing risk, radically simplifying IT operational complexity, and minimizing tasks performed by end-users. For detailed information see [Cisco Secure Access].

Google Chrome Enterprise overview



Chrome Enterprise brings organizations the secure and reliable browser employees love, with key management tools for IT and security teams. Organizations using Chrome Enterprise 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
The bridge to possible

Contents

Chrome Enterprise 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.

Combined private application process

The primary use-case of this joint solution is Cisco Secure Access serving sensitive private web applications to managed endpoints that have Chrome Enterprise as their enterprise browser.

Cisco's Zero Trust Network Access (ZTNA) uses least privilege principles, contextual insights, and client or clientless-based methods to deny access by default and allow access to apps when granted. And Chrome Enterprise ensures that users and the data they accessed from within Managed Chrome Browsers are protected.

End-user experience

Sample.com has deployed Cisco Secure Access to ensure secure access for their end users to their internal Jira ticketing system. Cisco Secure Access agents are deployed onto their managed endpoints and Chrome Enterprise has been deployed as their Secure Enterprise Browser.

Sample.com also ensures that Chrome Enterprise is the only browser deployed on these managed endpoints - they can do this using popular MDM/UEM tools.

chrome enterprise

CISCO
The bridge to possible

Contents

Paula, an employee at sample.com, opens their Managed Chrome Browser and types jira.sample.com. Cisco Secure Access assesses the device posture and provides access to Paula. Because Secure Access uses the MASQUE protocol to proxy web traffic, only the intended traffic dictated by the customer's policy is intercepted; everything outside of that policy flows directly to the Internet.

Based on the policies that the sample.com administrator has setup, Paula sees a watermark when jira.sample.com is opened in Chrome. Additionally, any data that Paula uploads or downloads via Chrome is scanned for sensitivity or maliciousness. Enterprise policies make sure no malicious or unvetted extensions can modify jira.sample.com. And finally, 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: Getting started.

Configure Cisco Secure Access

1. **Get Started with Cisco Secure Access:** At a high level you'll begin by provisioning your organization's network connections, users, and groups, and set up integrations with SAML Identity Providers (IdPs). The first step is ensuring access to the Secure Access dashboard.
   - Sign in to Secure Access with Single Sign-On (SSO) Security Cloud sign-on.
2. **Enable Network Infrastructure and Connections:** Deploy your resource connector groups, resource connectors, and tunnel groups to establish tunnels to Secure Access from your private applications. You can choose to use resource connectors for automated onboarding of application access, build IPSec tunnels to on-premises data centers or connections secured by Zero Trust Network Access.
   - For detailed instructions on setting up network connectors and network tunnel groups, see the documentation here.

chrome enterprise

CISCO
The bridge to possible

Contents

3. **Configure Private Resources:** You'll start by setting up private resources which include private subnets and applications deployed and managed by your organization.
   - For detailed instructions on setting up private resources, see documentation here.
4. **Configure End User Connectivity:** Zero trust-based traffic steering will allow you to define the granularity of your access controls and traffic flows connecting to private resources from user devices.
   - For detailed instructions on setting up users and groups, see the documentation here and follow the instructions specific to your identity provider.
5. **Configure Endpoints:** You'll begin by provisioning and setting up the Cisco Secure Client. Once provisioned you'll be able to manage Zero Trust Access on the Cisco Secure Client.
   - Download Cisco Secure Client from the Cisco Secure Access dashboard: Connect > Cisco Secure Client
     - Select OS version(s) to download.
     - For detailed instructions on setting up the Zero Trust Access module in Secure Client, see documentation here.
6. **Configure Intrusion Prevention System (IPS):** Intrusion Prevention System (IPS) helps prevent attacks on your private resources.
   - Detailed setup instructions are available here.
7. **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
The bridge to possible

Contents

Configure Chrome Enterprise

- **Start with Chrome Enterprise Core (previously named Chrome Browser Cloud Management):** 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:** Empower yourself with Chrome Enterprise 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's Security Reporting to gain valuable insights into potential threats Google Workspace users may encounter while browsing. Once Security events 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
The bridge to possible

Contents

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 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
The bridge to possible

Contents

- 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 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, deployed alongside 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 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
The bridge to possible

Contents

- **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

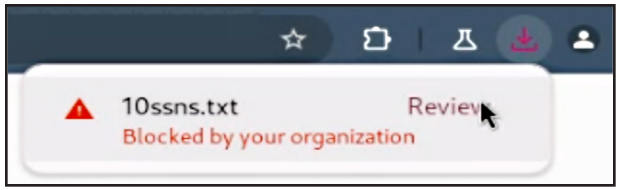
- **Step 1:** Set up Chrome browser Enterprise connector policies. Go to Set Chrome Enterprise connector policies for Chrome Enterprise in Google Chrome Enterprise Help for details.
- **Step 2:** Set up data protection rules in Google Workspace Admin console.
- **Step 3.** Set up activity alerts. Go 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 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

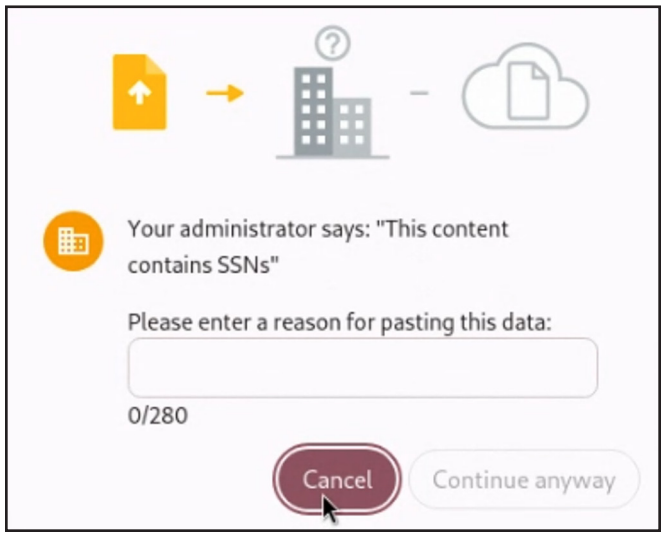
CISCO
The bridge to possible

Contents

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'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
The bridge to possible

Contents

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

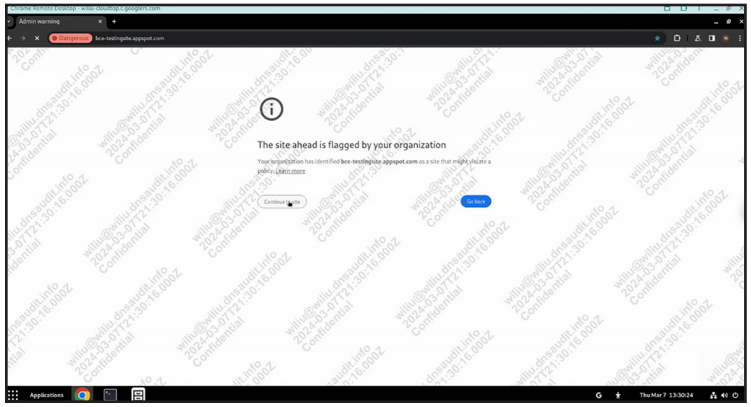
Data exfiltration can also happen through printing sensitive documents from enterprise applications. Chrome Enterprise's printing data protection rules provide precise control to mitigate this risk:

- **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 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
The bridge to possible

Contents

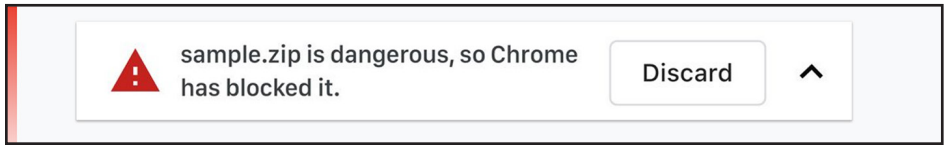
Threat protections

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 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, 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.

chrome enterprise

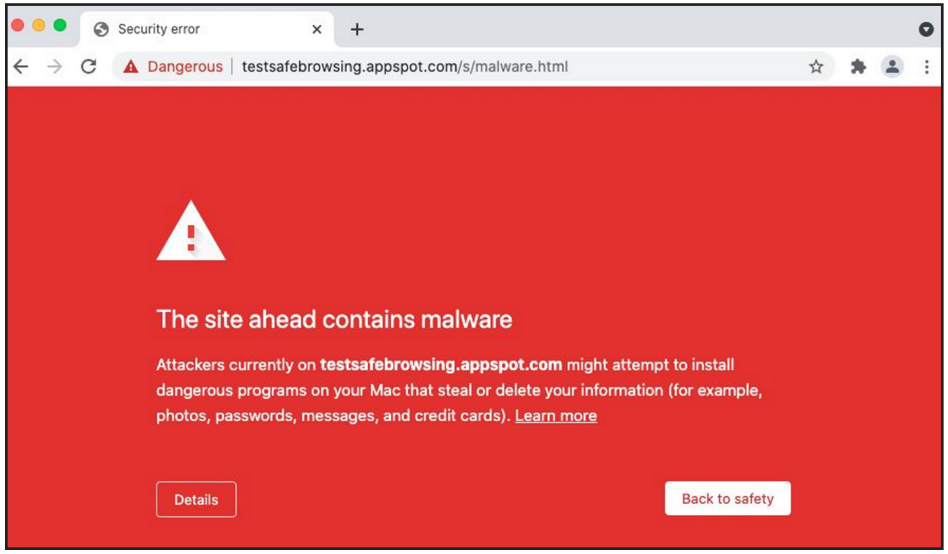
CISCO
The bridge to possible

Contents

Phishing protections

Chrome Enterprise 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.

chrome enterprise

CISCO
The bridge to possible

Contents

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 deployed can also use enterprise policies in order to prevent extensions from altering Private Web Application pages served via Cisco Secure Access.

Advanced device trust

Cisco Duo provides an integrated solution to provide advanced device trust for the full workforce.

For detailed information see Manage Chrome Enterprise device trust connectors.

C07-4435933-00 06/24