Cisco Cloud Web Security Chrome Extension Administrator Guide

First Published: June 27, 2016
Last Updated: September 8, 2016

Conventions

This document uses the following conventions.

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier font`	Terminal sessions and information the system displays appear in `courier` font.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: **Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.**

Overview

The Cisco Cloud Web Security (CWS) Chrome Extension allows you to configure your Chrome OS devices (such as Chromebook and Chromebox) to redirect web traffic to Cisco's CWS service. This allows you to protect and inspect web traffic, enforce policy, and gather analytics on web usage on your Chrome OS devices. The solution is delivered as a Chrome browser extension that can be silently deployed by a system administrator to the device with no end user involvement. There is nothing for the user to configure. The extension provides seamless web security for the Chrome browser.

In the CWS Chrome Extension, the following features are available:

- Traffic redirection to the CWS service for HTTP and HTTPS traffic
- Reporting and analytics
- Warn, block, authenticate, and anonymize policy rules
- HTTPS inspection (optionally decrypt and secure HTTPS traffic)
- Malware scanning in the cloud
- SafeSearch and SearchAhead for supported search engines
- User identity from the user's Google account
- SAML and Clientless Authentication (using cookie surrogates)
- Cloud Bypass/Whitelisting (define a list of IP ranges and/or domains for which requests should not go through the CWS proxy)
- Trusted Network Detection (disable the CWS Chrome Extension when on-premises to leverage the security of an on-premises connector appliance)
- Secondary failover proxy (secondary CWS proxy available for redundancy)

Supported Devices and Operating Systems

The CWS Chrome Extension is supported on:

- Chrome OS devices, such as Chromebook and Chromebox, running version 52 or newer.

The CWS Chrome Extension is *not* supported on:

- Chrome browser on OS X, Windows, and Linux.
- Devices running variations or third-party distributions of Chrome OS, such as Neverware CloudReady.

Additionally, in order to deploy the CWS Chrome Extension, a Google Apps for Work or Google Apps for Education subscription is required. For each Chrome OS device that you wish to deploy the extension on, you must also have a Chrome Management license. Cisco does not provide, support or sell subscriptions to these services. For more information, contact your Google sales representative, or see https://www.google.com/work/chrome/management-console/.

Note: For correct operation of the CWS Chrome Extension, we recommend that certain Chrome OS policies are applied to your target devices. For instance, you should ensure that there are no explicit proxy settings configured on the device. Otherwise, the explicit proxy could conflict with the CWS Chrome Extension. For more information, see Recommended Chrome OS Policies. Additionally, if you have a connector appliance on your on-premises network (such as an ISR, ASA, WSA, or CWS Standalone Connector), you may have to complete some extra steps to ensure compatibility. For more information, see Compatibility with Other Connectors.

Provisioning and Deployment

The CWS Chrome Extension is hosted unlisted on Google's Chrome Web Store. To find the extension on the web store, you need the extension's unique identifier. If you have not received this identifier, please contact your account manager. Automatic updates are handled though the Chrome Web Store extension management process.

Deployment of the CWS Chrome Extension involves using the Google Apps for Work or Education console to search and locate the **CWS Chrome Extension** in the Chrome Web Store. The following section describes how to configure the CWS Chrome Extension.

Configuration

The CWS Chrome Extension is configured through a JSON file containing key and value pairs which determine the behavior and functionality of the extension.

For most configuration options, if you do not specify an option or specify an invalid value, the extension uses a default value instead. See the Configuration Properties table below for information on which options are available and their default values. Note that some options, such as the license key and proxy host, are mandatory. If you do not specify a correct value for a mandatory configurable option, all web traffic on the Chrome OS device gets blocked until either a correct configuration is provided or the extension is removed.

Below is an example of the configuration JSON file that is required to configure the CWS Chrome Extension. Use this example in conjunction with the Configuration Properties to customize a configuration file that suits your needs.

```
{
"LicenseKey": {
"Value": "ABCDEFGHIJKLMNOPQRSTUV1234567890"
},
"ProxyHost": {
"Value": "access123.chrome.cloudsec.cisco.com"
},
"SecondaryProxyHost": {
"Value": "access345.chrome.cloudsec.cisco.com"
},
"TNDHost": {
"Value": "https://yourinternalserver.com"
},
"TNDCheckIntervalMinutes": {
"Value": 1
},
"WhitelistEnabled": {
"Value": true
},
"WhitelistCheckIntervalMinutes": {
"Value": 60
},
"UserIdentityEnabled": {
"Value": true
}
}
```

Note: If the user visits `chrome://policy` in the Chrome browser on their device, they can see the contents of the JSON configuration file but cannot modify it. This is due to the way Google Chrome handles managed extension configurations. This means that the user can see the CWS license key it is configured with. For this reason, we strongly recommended that you use group keys which you can revoke and reissue, if necessary.

Configuration Properties

The table below outlines each configuration option in the CWS Chrome Extension JSON file. If you wish to have a different configuration per organization (for example, a different group key), you may create multiple JSON files per organization you have configured under your Google Apps for Work or Google Apps for Education account.

For the **ProxyHost** and **SecondaryProxyHost** configurable options, you must specify a proxy host ending in `.chrome.cloudsec.cisco.com`.

If for other connectors your primary tower is **`access123`**`.cws.sco.cisco.com`, you should use **`access123`**`.chrome.cloudsec.cisco.com` here.

If your tower is of the form `proxy123.scansafe.net`, these proxies are not supported. Contact your Cisco account manager for assistance.

Property	Default	Description
LicenseKey	None	**Mandatory.** Your CWS license key. This may either be a company key, or if you wish to apply a group policy, a group key. For example, `"ABC12345678"` in quotes.
ProxyHost	None	**Mandatory**. Your proxy host ending in .chrome.cloudsec.cisco.com (as described above). For example, `"access123.chrome.cloudsec.cisco.com"` in quotes.
SecondaryProxyHost	None	Your secondary or backup proxy host ending in .chrome.cloudsec.cisco.com (as described above). For example, `"access123.chrome.cloudsec.cisco.com"` in quotes.
WhitelistEnabled	`false`	The word `true` or `false` (without quotes) either enabling or disabling whitelist/cloud bypass functionality. For more information, see the Cloud Bypass (Whitelisting) section.
WhitelistCheckIntervalMinutes	`60`	A number in minutes representing how often the extension should check for whitelist updates from the CWS server. Minimum value is 1. For more information, see the Cloud Bypass (Whitelisting) section.
UserIdentityEnabled	`false`	The word `true` or `false` (without quotes) either enabling or disabling user identity from the account signed in to the Chrome OS device. For more information, see the User and Group Identity section.

TNDHost	None	A hostname beginning with https:// that gets queried to determine whether the device is on a trusted network. If no value or an empty string is provided, the trusted network detection functionality is disabled. For example, `"https://intranet.local/example.htm"` in quotes. For more information, see the Trusted Network Detection section.
TNDCheckIntervalMinutes	1	A number in minutes representing how often the extension should poll the trusted network detection host to determine whether the device is on a trusted network. Minimum value is 1. For more information, see the Trusted Network Detection section.

Note: If you already have the CWS Chrome Extension deployed with a valid configuration file, and you attempt to make changes and the new configuration file is invalid (for example, missing a specified value or invalid values for the mandatory configuration parameters), the new configuration file is not validated and the existing configuration file remains in use. If the new configuration file has valid values for the mandatory configuration parameters, default values are used for the non-mandatory configuration parameters if the new values for these parameters are not valid.

Deployment through Google Apps for Work or Education

In order to deploy the CWS Chrome Extension, a Google Apps for Work or Google Apps for Education subscription is required. For each Chrome OS device that you wish to deploy the extension on, you must also have a Chrome Management license. Cisco does not provide, support, or sell subscriptions to these services. For more information, contact your Google sales representative, or see https://www.google.com/work/chrome/management-console/.

Once you have your JSON configuration file ready, you can deploy the extension to one or more organizations through the Google Apps for Work or Education console.

To deploy the extension, complete the following steps:

1. Log in to your Google Apps for Work or Education console.
2. Click the **Device Management** icon.

3. Under **Device Settings** in the menu to the left of the screen, select **Chrome Management**.
4. You are taken to the Chrome Management page. Now select **App Management**.
5. In the left side panel, enter the **unique identifier** for the CWS Chrome Extension in the **Find or Update Apps** search box. Press the **Search** button.
6. In the results list, click on **CWS Chrome Extension**.
7. You are taken to a page where you can configure the extension. Select **User settings**.
8. Now, for each organization you wish to deploy the CWS Chrome Extension, select it under the Orgs menu. Toggle **Force installation** to on, and upload the JSON configuration file for that relevant organization. Then select **Save**.
9. Once you have completed these steps, the extension and configuration should be silently pushed to the target Chrome OS devices within minutes. If you uploaded the extension to an internal server, ensure the Chrome OS device is switched on and connected to your corporate network. If the extension still does not appear, try rebooting the device.

For more information on how to manage Chrome extensions, contact your Google support representative or see https://support.google.com/chrome/a/answer/1375694?hl=en.

If you wish to update the configuration after deployment, you can upload a new configuration file using the Google Admin Console, as you did when performing the initial deployment. In most cases, the CWS Chrome Extension detects and updates the configuration accordingly within a few minutes. In some cases, the user may have to log out and back in to the Chrome OS device for the changes to take effect.

Compatibility with Other Connectors

The CWS Chrome Extension protects your Chrome OS devices without requiring any on-premises connector. However, you may have an on-premises connector which redirects traffic to CWS, such as the Web Security Appliance (WSA), Adaptive Security Appliance (ASA), Integrated Services Router (ISR), or CWS Standalone Connector. If you have such a connector, some configuration may be required to ensure the CWS Chrome Extension cooperates with the connector and behaves as expected.

Integrated Services Router (ISR) and Adaptive Security Appliance (ASA)

Both the ISR (including the ISR 4000 Series) and ASA connector appliances redirect traffic to CWS without additional configuration on the user devices. Proxied traffic from the CWS Chrome Extension may be proxied again by your connector appliance. This could lead to “double proxying” which could degrade performance or cause undesired or undefined behavior.

The easiest way to prevent this is to use the Trusted Network Detection feature of the CWS Chrome Extension. This allows the CWS Chrome Extension to detect when you are on-premises and temporarily

disable the proxying functionality of the extension, so that the ISR or ASA provides CWS functionality instead. For more information, see the Trusted Network Detection section.

If you do not wish to use Trusted Network Detection, you can whitelist the proxy host used in the CWS Chrome Extension on your ISR 4000 Series. This prevents the connector from attempting to "double proxy" the traffic. For instance, if your proxy host is `access123.chrome.cloudsec.cisco.com`, we recommend you whitelist this host on port 443. For more information, see the product support documentation for your particular connector appliance.

For the ISR G2 and ASA, domain-based whitelisting is not supported for HTTPS traffic. All requests originating from the CWS Chrome Extension are sent through a secure HTTPS tunnel. Although Trusted Network Detection is preferred, another option available to you is to whitelist the IP ranges used by your towers. For information about the IP ranges for your datacenter and instructions on how to whitelist these IP ranges on your connector appliance, contact your Cisco support representative.

Web Security Appliance (WSA) and CWS Standalone Connector

Both the WSA in non-WCCP mode and CWS Standalone Connector require you to set the proxy setting on any user agents; for example, web browsers. If you do not set the proxy, the traffic does not get redirected to CWS through the connector. As the CWS Chrome Extension redirects traffic to CWS, no configuration or extra steps are required for interoperability with the WSA and CWS Standalone Connector, as long as you do not manually set a proxy on the Chrome OS devices.

When using an ASA to perform WCCP redirection to a WSA that is configured for connector mode, the WSA WCCP forwarding and return methods must be set to allow L2 only.

Note: If you have a firewall or other appliance that selectively blocks web traffic, ensure requests to your proxy host can pass through the firewall. This can be achieved, for instance, by whitelisting your proxy host in the firewall configuration. Contact your firewall vendor for information on how to achieve this.

User and Group Identity

The CWS Chrome Extension supports multiple methods with which you can identify the user and groups of users. Group identity allows you to apply different policies depending on the group a user belongs to. For example, you could have a different set of web filters for teachers and students in an educational organization. Additionally, user identity allows you to pinpoint the traffic originating from a specific user for the purposes of analytics and reporting from Cisco ScanCenter, the configuration portal to CWS.

Note: Currently, CWS does not support user license keys for policy at the individual user level. Instead, you can add your users to a group and then apply a group policy.

Chrome OS Account and Groups

If your organization makes use of managed or supervised users for your Chrome OS devices (for example, if your users sign in to the Chrome OS device using a Google account or Active Directory account), then the CWS Chrome Extension can leverage this information for user identity. When this feature is enabled, the email address of the user is sent with every request and is visible in reports in Cisco ScanCenter. Only the email address is reported; no group information is sent.

By default, this feature is disabled. To enable this feature, ensure that the **UserIdentityEnabled** flag in the configuration file is set to true. For more information, see the Configuration section.

If you wish to also use group identity and apply group-based policies, we recommended that you either:

- Configure the Chrome OS device with a group license key as well as leveraging the Chrome OS user identity. For more information on how to configure the Chrome OS device with a group key, see the Configuration section.
- Create a custom group within Cisco ScanCenter, and add the associated user email addresses to the custom group. For more information on custom groups, see the Cisco ScanCenter Administrator Guide.

If you wish to verify that user/group identity is being correctly reported, browse to http://whoami.scansafe.net. The **authUserName** field on this page should be populated with the email address of the Chrome OS profile.

Note: If you set **UserIdentityEnabled** to `true` and also make use of Clientless Authentication or SAML, any user identity from Clientless Authentication or SAML overwrites the user identity obtained from the Chrome OS user profile.

SAML and Clientless Authentication

The CWS Chrome Extension supports SAML and Clientless Authentication functionality. To enable SAML/Clientless Authentication functionality, configure authentication rules and link your LDAP/AD server in Cisco ScanCenter. For more information, see the Cisco ScanCenter Administrator Guide.

Note: Only cookie surrogates are supported for SAML/Clientless Authentication. IP surrogates are not supported.

Policy and Auditing

CWS web filtering functionality, such as warn, block, and authenticate policies, is supported for Chrome OS devices using the CWS Chrome Extension.

To define the web filtering policies that are applied to devices using the CWS Chrome Extension, use the same Cisco ScanCenter user interface that you use for all of your other connector appliances. Refer to the Cisco ScanCenter Administrator Guide for instructions on how to use the web filtering functionality and how to configure policies.

HTTPS Inspection

The CWS Chrome Extension supports HTTPS Inspection functionality. HTTPS Inspection allows you to decrypt HTTPS traffic and apply policy, scan the traffic for malware, and gather reporting metrics. You can define which domains, IP addresses, and categories of HTTPS traffic get inspected. These policies are configured in Cisco ScanCenter.

In order for the HTTPS Inspection functionality to work, you must first set up a Certificate Authority (CA) in Cisco ScanCenter. Since Chromebooks only support certificates in PEM format, the certificate generated using or uploaded to the ScanCenter portal can be converted from CRT to PEM format using the following command:

```
openssl x509 -inform DER -outform PEM -text -in certificateName.crt -out certificateName.pem
```

Once the conversion is done, install the PEM CA certificate on all Chrome OS devices where the HTTPS Inspection policy is being applied. The Google Apps for Work or Education consoles provide a mechanism for deployment of trusted CA certificates to devices within an organization. For more information, see https://support.google.com/chrome/a/answer/3505249?hl=en&ref_topic=3504941, or contact your Google support representative. When installing the certificate via the Google Apps for Work or Education consoles, make sure to select the **Use this certificate as an HTTPS certificate authority** check box.

Google advises that certain Google-owned or Google-affiliated domains are exempted from any SSL decryption processes, such as the HTTPS inspection functionality provided by CWS. The list of domains can be found on Google's support pages at https://support.google.com/chrome/a/answer/6334001?hl=en&ref_topic=3504941.

Note: This list changes from time to time. We recommend that you ensure the domains included in this list are not included in any HTTPS inspection policy. If you have a HTTPS inspection policy that decrypts all HTTPS traffic or decrypts categories of traffic that may clash with the above domains, you can add the domains as exceptions. For more information, see the Cisco ScanCenter Administrator Guide.

Reporting

CWS provides reporting functionality through Cisco ScanCenter, enabling you to analyze the web traffic of your users. This reporting functionality also includes all traffic originating from your Chrome OS devices. You can run the same type of reports that you run for other CWS connectors. For more information, see the Cisco ScanCenter Administrator Guide.

If you wish to create reports specifically for your Chrome OS devices, create a filter on the **Connector Version** attribute. In the filter, include a **starts with** operator with a value of **ChromeExtension**. Applying this filter to your reports displays the traffic originating from your Chrome OS devices.

If you wish to report on user identity, you have two options. You can either leverage Clientless Authentication/SAML functionality to retrieve identity from your LDAP or Active Directory server, or you can use the identity of the Chrome OS profile. For more information, see the User and Group Identity section.

Cloud Bypass (Whitelisting)

The cloud bypass or whitelisting functionality allows you to define domains and/or IP ranges for which the traffic does not get proxied through the CWS service. Requests to domains and/or IP ranges on the whitelist are sent directly to the Internet. For instance, you could whitelist your internal web servers, such as a corporate intranet, to ensure your users can access these resources without the request traversing the CWS proxy. The whitelist is hosted in the cloud and configured through Cisco ScanCenter. The CWS Chrome Extension periodically retrieves the whitelist.

The CWS cloud bypass functionality is also supported on the ISR G2 and ISR 4000 series connectors, as well as the CWS Mobile Browser for iOS and Android. Cloud bypass rules created for these connectors and applications can be shared with the CWS Chrome Extension if desired.

Cloud Bypass Configuration

In order to enable the cloud bypass functionality, you must set the **WhitelistEnabled** flag in the CWS Chrome Extension configuration file to `true`. If the value is `false` or missing, the CWS Chrome Extension does not attempt to pull new whitelist changes and does not apply any previously downloaded whitelist.

By default, the CWS Chrome Extension pulls cloud bypass rules from CWS every 60 minutes. The cloud bypass retrieval frequency can be configured by changing the **WhitelistCheckIntervalMinutes** property in the CWS Chrome Extension configuration file. The minimum value for this property is 1, representing a cloud bypass rule fetch every one minute. For more information on how to configure the CWS Chrome Extension, see the Configuration section.

Supported Rule Types

The CWS Chrome Extension supports a subset of the CWS cloud bypass rule format. The following rule types are supported:

- Domain names, optionally with wildcards (for example, `cisco.com`, `meraki.cisco.com`, `*opendns.com`)
- Destination IP ranges with subnet mask (for example, `192.168.0.0/255.255.0.0`)

Note: Source IP ranges, user-agent headers, regular expression and other special characters other than “*” (such as “?”, “^”, “[”, “]”, “{”, “}”, “(”, “)”, “$”, “/”, “\”) and domain names of more than 256 characters are

not supported by the CWS Chrome Extension. If your cloud bypass list contains any of these unsupported rules, they get silently ignored. For more information about configuring cloud bypass lists, see the Cisco ScanCenter Administrator Guide.

Note: Any domain rule added in a cloud bypass list that matches the `cwsuploads.sco.cisco.com` or `407.cws.cisco.com` domains do not get used to whitelist traffic on the Chrome OS device. This includes rules with wildcards that match these domains, such as `*cisco*` or `*sco.cisco.com`. Requests to these domains must traverse the CWS service for correct operation of the CWS Chrome Extension. Any rule that matches these domains is ignored.

Trusted Network Detection

The Trusted Network Detection (TND) functionality allows you to configure the CWS Chrome Extension to know when it is on what you define as a trusted network (for example, your on-premises corporate network). When the CWS Chrome Extension detects it is on such a network, it does not redirect traffic to CWS and instead sends traffic directly to the Internet. If you make use of certain on-premises connector appliances, such as an ISR or ASA, you may need to enable TND functionality to ensure compatibility with these appliances. For more information, see the Compatibility With Other Connectors section.

TND is configured by specifying a HTTPS server that the CWS Chrome Extension can attempt to access. This server should be an internal web server, such as an HTTPS intranet site, that is not accessible outside of the trusted network. The CWS Chrome Extension periodically attempts to access this server, and if a connection can be successfully established, the CWS Chrome Extension knows it is on a trusted network and proxying is disabled. The next time your HTTPS server is queried, proxying is re-enabled if your HTTPS server has become unreachable (for example, if the user has roamed off premises).

The CWS Chrome Extension treats the network as trusted, and the proxy is disabled, if all of the following conditions are met:

- A connection can be established with the TND host.
- A TLS handshake can be completed with the TND host. This means that the TND host must serve a valid certificate that Google Chrome trusts.
  - The certificate must not have expired.
  - The common name (CN) of the certificate must match the TND host.
  - The certificate must be signed by a certificate authority (CA) that Google Chrome trusts. If your certificate is self-signed, then the issuing CA must be imported into the Google Chrome trust store.
- After the TLS handshake, the TND host must respond with a successful HTTP response code. A successful HTTP response code is one within the 200-299 range inclusive.

Set the HTTPS server you want to use for TND in the CWS Chrome Extension using the **TNDHost** property. If no TND host is given, TND functionality is disabled. Set the frequency for which the TND host is tested using

the **TNDCheckIntervalMinutes** property, which has a default value of 1. For more information, see the Configuration section.

Note: If you specify a TND host that does not specify a protocol, or specifies a protocol other than HTTPS such as HTTP or FTP, the host is ignored and TND functionality is disabled.

Proxy Failover

The **SecondaryProxyHost** configuration option allows you to specify a backup CWS proxy that the CWS Chrome Extension uses to proxy traffic through the CWS service in case of errors using your main proxy host.

As with **ProxyHost**, for **SecondaryProxyHost** you must specify a proxy host name ending in `.chrome.cloudsec.cisco.com`.

If for other connectors your secondary tower is `access123.cws.sco.cisco.com`, you should use `access123.chrome.cloudsec.cisco.com`.

If your tower is normally in the form of `proxy123.scansafe.net`, these proxies are not supported. Contact your Cisco account manager for assistance.

Note: When the CWS Chrome Extension uses your backup CWS proxy during a failover, it periodically attempts to reconnect and use your primary CWS proxy again.

Captive Portals

For the CWS Chrome Extension to work with captive portals, add the following domains to the whitelisted domains:

- "`.*gstatic.com`" domain
- Domains of the captive portals you wish the extension to support

For information on how to enable and configure Cloud Bypass whitelisting functionality, see the Cloud Bypass (Whitelisting) section.

Recommended Chrome OS Policies

To ensure correct operation of the CWS Chrome Extension, and to ensure that the user cannot modify or interfere with the extension, there are several Google Chrome enterprise policies that should be enabled. Use the Google Apps for Work or Education console to enable these policies for your users.

For information on how to configure Chrome OS policies, see the Google documentation at https://support.google.com/chrome/a/answer/2657289?hl=en, or contact your Google support representative.

Access the Google Chrome policy configuration by following these steps:

1. Log in to the Google Admin Console.
2. From the Admin Console, select **Device Management**.
3. In the menu on the left of the screen, select **Chrome Management**.
4. Select **User Settings**.
5. On the left, select the organization you wish to configure.

The recommended policies are as follows:

- **User Experience > Developer Tools**
  - Disable by selecting the **Never allow use of built-in developer tools** option.
  - This ensures that your users cannot open Chrome's developer tools to manipulate the state of the CWS Chrome Extension.
- **Network > Proxy Settings**
  - Select the **Allow user to configure** option.
  - This allows the CWS Chrome Extension to manage the Chrome OS proxy configuration.
  - Once the CWS Chrome Extension is installed on the device, the user cannot change the proxy, despite the name of the value of this setting.
  - If this setting is set to any other value, the CWS Chrome Extension may not function as expected.
- **Network > Data Compression Proxy**
  - Disable the user's ability to select data compression by selecting the **Always disable data compression proxy** option.
  - The data compression function provided by Google Chrome acts as a web proxy. If the data compression proxy is enabled, it may conflict with the CWS Chrome Extension and result in unexpected or undefined behavior.
- **Apps and Extensions > Allow or Block All Apps and Extensions**
  - Select **Block all apps and extensions except the ones I allow**.
  - Blocking all extensions and applications except the ones you explicitly allow ensures that conflicting programs (for example, proxy or VPN extensions) cannot be installed by the user to circumvent the CWS Chrome Extension.

- **Security > Incognito mode**
  - Disable by selecting the **Disallow incognito mode** option.
  - By default, the CWS Chrome Extension does not operate in incognito mode unless the user explicitly opts in to run the extension in this mode. This is due to Google Chrome policy limitations and cannot be overridden by enterprise policy. Therefore, we recommend disabling incognito mode.

Troubleshooting and Logging

The CWS Chrome Extension generates log messages which can be used to analyze and debug problems with the extension. These log messages are sent to the Google Chrome console within the Developer Tools interface. Ensure that you enable the Developer Tools on only the device you are using for troubleshooting, not on all of your user devices.

To gather these troubleshooting logs, follow these steps:

1. Temporarily enable Chrome's Developer Tools if your Chrome OS policy has disabled it.

   Note: We recommend you keep Chrome's Developer Tools disabled for security purposes. However, in order to gather debug logs, you need to temporarily re-enable this functionality.

2. Open Google Chrome on the Chrome OS device and reproduce the issue.
3. From the Google Chrome menu, select **More Tools** and then select **Extensions**.
4. The extensions page opens. In the top right of this page, select **Developer mode**.
5. Under the Cisco Cloud Web Security extension, click the **html/background.html** link under **Inspect Views**.
6. Developer tools opens. Select the **Console** tab.
7. You can now see the CWS Chrome Extension debug logs. To save them, right click any of the log messages and select **Save as**.

If you require assistance with an issue, contact your Cisco support representative and provide the troubleshooting logs.

Legal Information

Cisco Trademark

Cisco Copyright