How to Get and Configure the Barracuda Chromebook Security Extension

https://campus.barracuda.com/doc/49744111/

> This feature is available for the Barracuda Web Security Gateway 410 and 410 Vx and higher, running version 11.0 and above. Note that t he Barracuda Chromebook Security Extension does not support user/device pairing; it should be installed in any Chrome browser that a user logins into which is tied to their Google domain. The extension will be disabled if it detects that the device it was installed on is not running a Chrome OS.

With the Barracuda Chromebook Security Extension installed on Chromebooks, users are identified and policy is applied based on the user whether they are inside your network or accessing the Internet from a public or private network. For example, this feature provides security for students, even when they take their Chromebooks home. Additionally, user generated traffic is logged and recorded for reporting purposes, providing administrators insight into all user activity.

The extension provides:

- Enforcing of security policies provided by the Barracuda Web Security Gateway
- Control and visibility over both HTTP and HTTPS traffic, without sending any user generated traffic through the Barracuda Web Security Gateway
- Synchronizing of policy and report data between the Chromebook and the Barracuda Web Security Gateway

Note that the extension, *not* the Barracuda Web Security Gateway, applies block/allow policies for admin.google.com on the Chromebook.

The Barracuda Chromebook Security Extension is available from the Google Chrome Web Store at no cost, and can be configured in the Google Admin console. Follow the instructions below to get and configure the Barracuda Chromebook Security Extension.

Features supported on the Barracuda Web Security Gateway

In addition to the ability to block HTTPS sites, the extension supports these features:

With the Barracuda Web Security Gateway version 11.x:

- Content Filtering
- Domain Filtering
- Custom Categories
- Web Logs
- Exceptions (Limited to Content Filtering and Domain filtering)

- Reporting, limited to features listed here

Note that application blocking is supported through Chromebook Management (admin.google.com). The following do not apply for Chromebook web traffic with the extension installed:

- Settings on the **BLOCK/ACCEPT > Web App Control** page; i.e. block/allow for applications listed on the page.
- Settings on the **BLOCK/ACCEPT > Web App Monitor** page; i.e. social media content monitoring and suspicious keyword alerts.
- Interactive block pages, which allow for login bypass or temporary access tokens, for example.

With the Barracuda Web Security Gateway version 12.x:

- All the features supported by the Barracuda Web Security Gateway 11.x
- Chromebook Granular Controls:
    - Option to set the frequency with which the extension attempts to sync traffic log data with the Barracuda Web Security Gateway.
    - Option to set the frequency with which the extension attempts to fetch and sync policy changes made by the administrator.
    - Option to configure Request Types to Filter - For example, not filtering stylesheets, images, or other object types reduces the processing load on the Chromebook.
- Time based policies
- Temporary Access Token features
- Google Directory Services

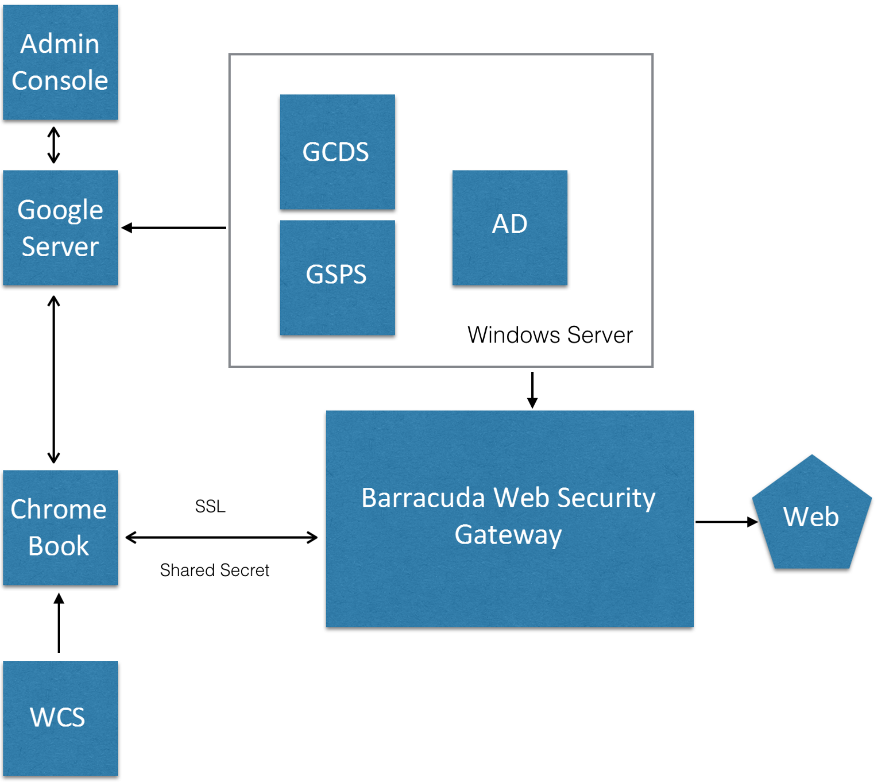
The following do not apply for Chromebook web traffic with the extension installed:

- Settings on the **BLOCK/ACCEPT > Web App Control** page; i.e. block/allow for applications listed on the page.
- Settings on the **BLOCK/ACCEPT > Web App Monitor** page; i.e. social media content monitoring and suspicious keyword alerts.

How the Barracuda Chromebook Security Extension Works

When installed on a Chromebook, the Barracuda Chromebook Security Extension queries the Barracuda Web Security Gateway for block/accept policies and applies them to all Chromebook web traffic. The extension is configured using the Google Admin console and can optionally use the Google Cloud Directory Sync (GCDS) and Google Workspace Password Sync (GSPS) to synchronize Chromebook user logins with the Barracuda Web Security Gateway for user-based exception policies.

If you do not configure GCDS/SSO, you can create local users with matching usernames, which will automatically match users coming from the google domains.



About web logs for Chromebook traffic

Unlike regular proxy traffic, Chromebook web traffic is not displayed immediately on the **BASIC > Web Log** page in the Barracuda Web Security Gateway web interface – it may take a few minutes for the log data display. If the Barracuda Web Security Gateway goes offline, and if the user already has the Barracuda Chromebook Security Extension installed, web traffic from that device will continue to be filtered based on the policies that were downloaded by the extension before the Barracuda Web Security Gateway went offline. In this scenario, the web logs are stored on the client machine and are displayed when the Barracuda Web Security Gateway is online again.

Authentication for Chromebook Users

For all Chromebook deployments, when using the Barracuda Chromebook Security Extension, configure Google Directory Services as the authentication service the Barracuda Web Security Gateway will use to apply policies to Chromebook users and groups. See How to Configure Google Directory Services for instructions.

Possible 'Permissions Error'

As a part of the security measure taken by Google, a new sign-in email alert may be sent to the Google account when configuring Google Directory Services on the Barracuda Web Security Gateway. Until the user confirms their new login in the Google **New Sign-In On Windows** alert pop-up, the **Test** button on the Barracuda Web Security Gateway on the **USERS/GROUPS > Authentication > New Authentication Service > Google Directory** tab displays "Permissions Erro".

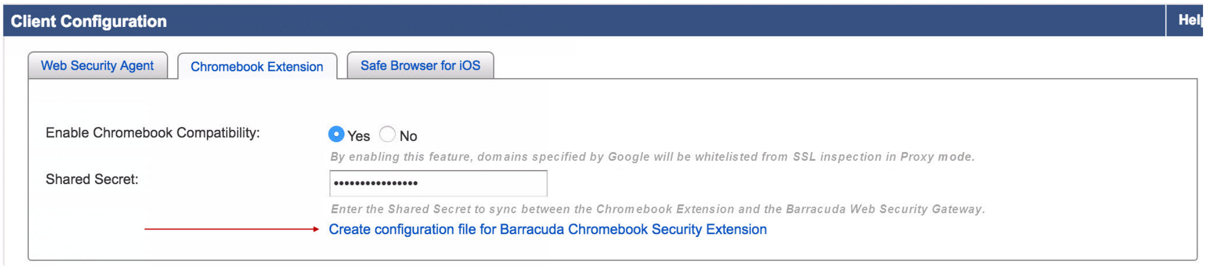
How to Download and Use the Barracuda Chromebook Security Extension

Step 1. Prepare the Chromebook configuration file using the Barracuda Web Security Gateway.

If Chromebooks are to be used outside of the network, you should use a domain name that resolves to the Barracuda Web Security Gateway both within and outside of the network. You may need to set up a DNAT rule on your firewall to forward port 8443 (or any other allowed port, preferably a unique port) traffic to the secure administration port on the Barracuda Web Security Gateway. Once the extension is installed, Chromebook logs and policy are synced and all communication is done via the secure admin port you configure.

Start by generating a text file that specifies the Barracuda Web Security Gateway you want your Chromebooks to sync with for security policies. To create the file:

1. Log into the Barracuda Web Security Gateway web interface as *admin* and go to the **ADVANCED > Remote Filtering** page.
2. In the **Client Configuration** section, click the **Chromebook Extension** tab and configure the following:
    1. Set **Enable Chromebook Compatibility** to **Yes.** Port 3128 is opened by default when this option is set to **Yes**.
    2. Create a shared secret, or password, which is used by the Barracuda Chromebook Security Extension on the Chromebook to communicate with this Barracuda Web Security Gateway. Do not use the "/" or "\" slash characters in the shared secret. It is important to use a text editor, such as Notepad, that does not add any markup to the text. For example: **17$k2Y4!** Enter in the **Shared Secret** field. Click **Save**.
    3. Click Create configuration file for Barracuda Chromebook Security Extension as shown below.



Enable Chromebook Compatibility: ● Yes ○ No

By enabling this feature, domains specified by Google will be whitelisted from SSL inspection in Proxy mode.

Shared Secret: ••••••••••••••••

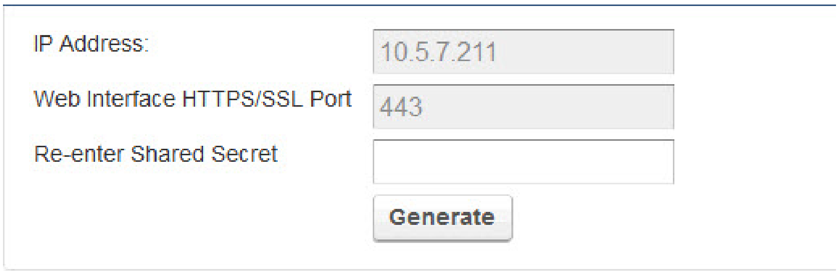
Enter the Shared Secret to sync between the Chromebook Extension and the Barracuda Web Security Gateway.

Create configuration file for Barracuda Chromebook Security Extension

3. You will see a popup with the required fields to generate the configuration file:

With the Barracuda Web Security Gateway version 11.0, the fields are as follows:

1. **IP Address -** This is the same as the **IP Address** on the **BASIC > IP Configuration** page.
2. **Web Interface HTTPS/SSL Port -** This is the same as the **Web Interface HTTPS/SSLPort** setting on the **ADVANCED > Secure Administration** page.
3. **Shared Secret -** Re-enter the shared secret you created on the **ADVANCED > Remote Filtering** page. Click **Generate**.



IP Address: 10.5.7.211

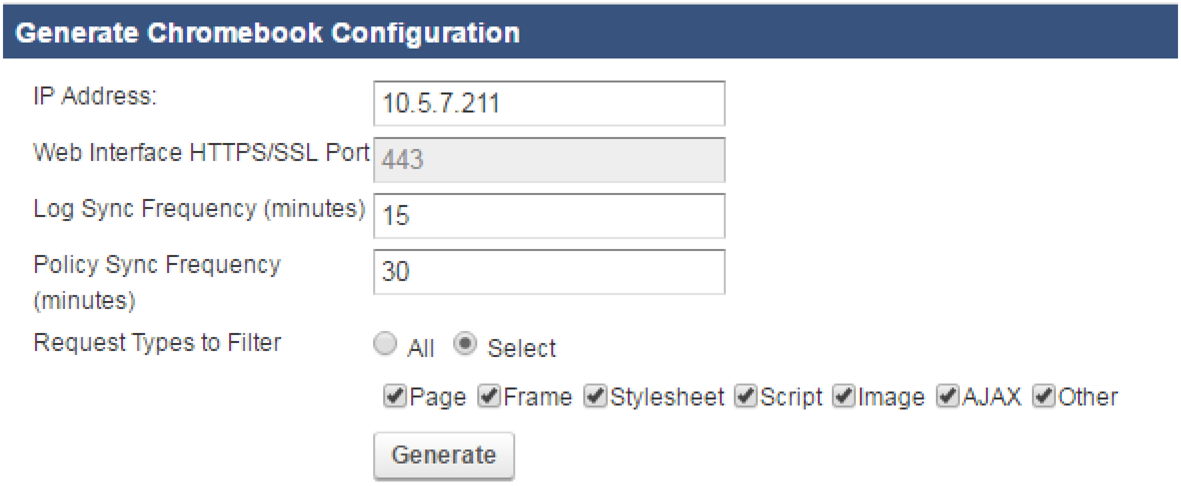
Web Interface HTTPS/SSL Port 443

Re-enter Shared Secret

4. Save the **chromebook_config.txt** file on your local system or network.

With the Barracuda Web Security Gateway version 12.x, the fields are as follows:

1. **IP Address -** This is the same as the **IP Address** on the **BASIC > IP Configuration** page.
2. **Web Interface HTTPS/SSL Port** - This is the same as the **Web Interface HTTPS/SSLPort** setting on the **ADVANCED > Secure Administration** page.
3. **Log Sync Frequency (minutes)** - Frequency with which the extension attempts to sync traffic log data with the Barracuda Web Security Gateway. Minimum setting should be 15.
4. **Policy Sync Frequency(minutes)** - Frequency with which the extension attempts to fetch and sync policy changes made by the administrator. Minimum setting should be 15.
5. **Request Types to Filter** - If you click **Select**, you will see options you can check for the extension to filter or not filter. For example, *not* filtering stylesheets or other object types reduces the processing load on the Chromebook.



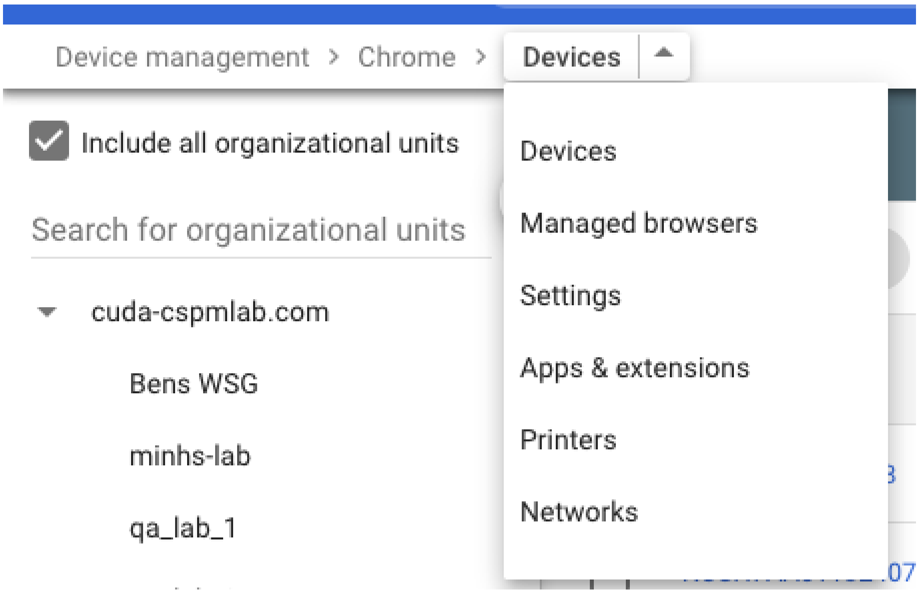
Generate Chromebook Configuration

IP Address:	10.5.7.211
Web Interface HTTPS/SSL Port	443
Log Sync Frequency (minutes)	15
Policy Sync Frequency (minutes)	30
Request Types to Filter	○ All ● Select
	☑Page ☑Frame ☑Stylesheet ☑Script ☑Image ☑AJAX ☑Other
	Generate

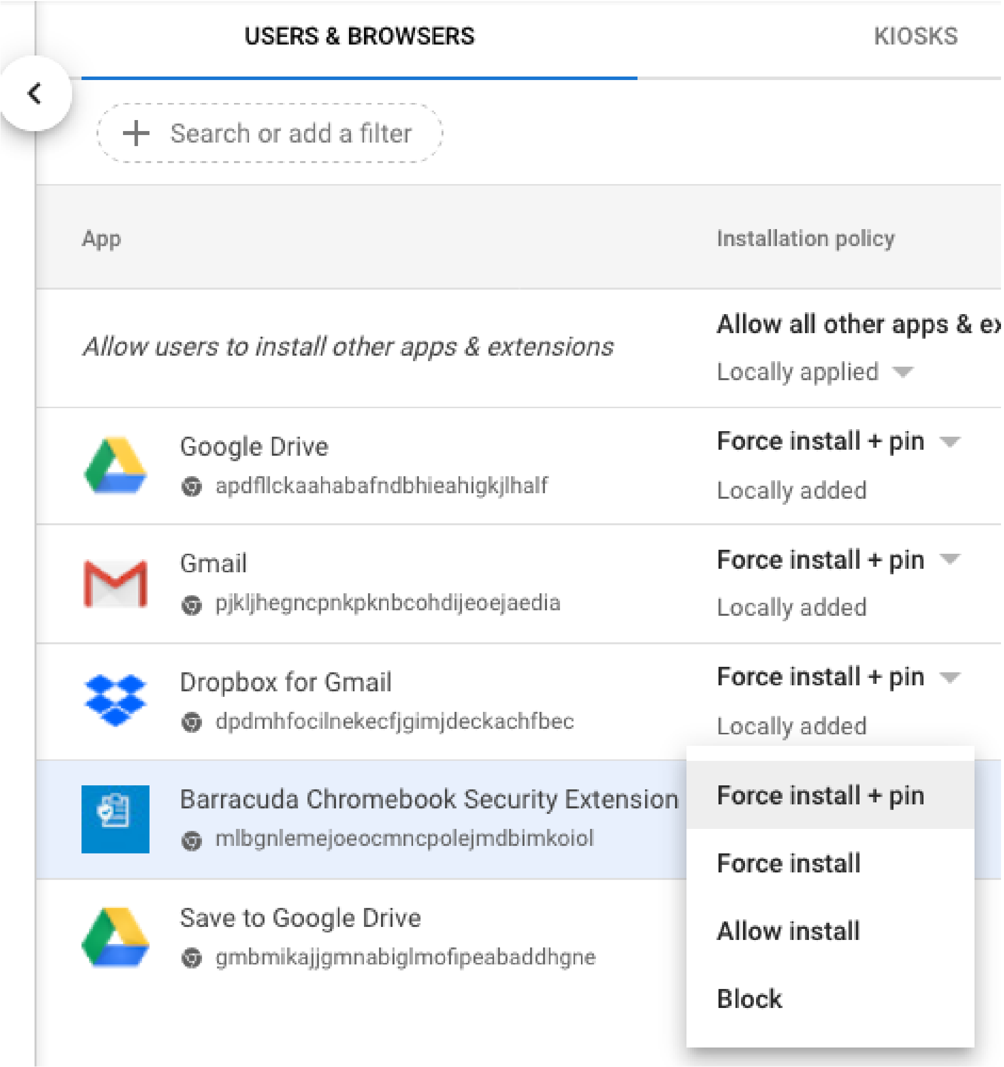
6. Click **Generate** to create the configuration file, and save the **chromebook_config.txt** file on your local system or network.

Step 2. Configure the Barracuda Chromebook Security Extension in the Google Admin console.

1. Log into Google Admin console as an administrator and add all managed devices per Google instructions here: Enroll Chrome devices.
2. Go to **Devices > Chrome Devices** and, using the **Devices** drop-down, select **Apps & extensions.**

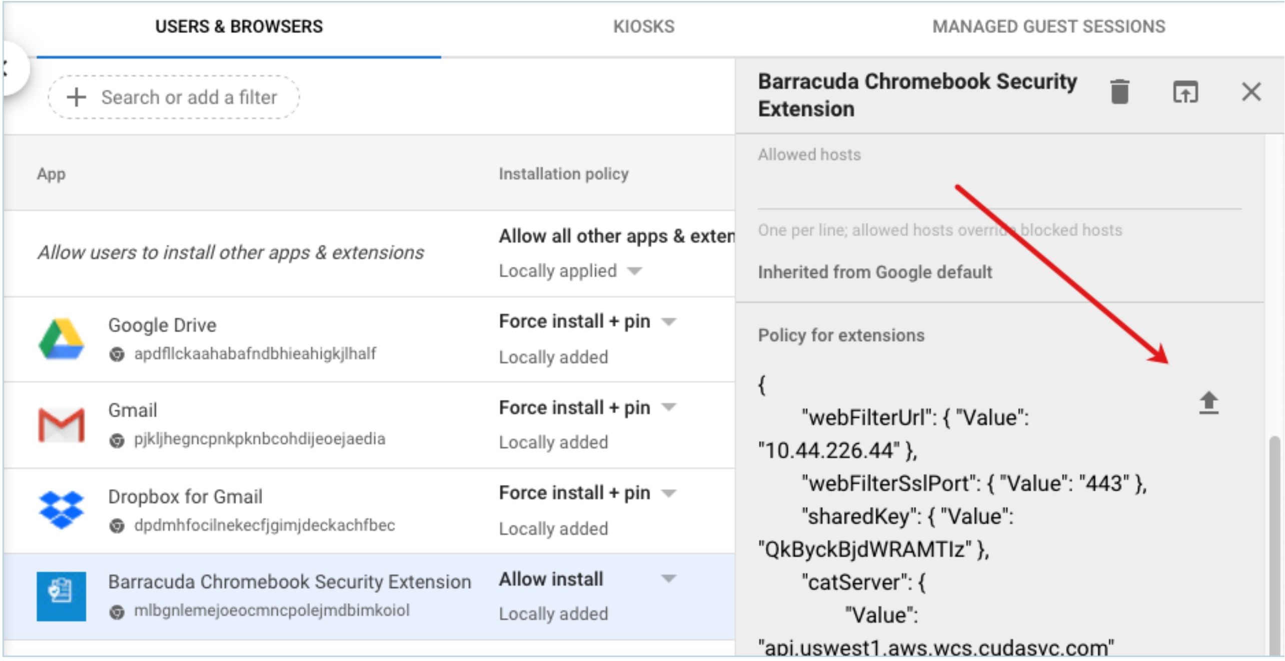


3. Click on **Barracuda Chromebook Security Extension** on the **Apps & extensions** page to configure the extension in the Google Admin console.
4. Click on the **Users & Browsers** tab. Modify the settings for: **Allow install**, **Force install**, and **Pin to taskbar** based on your setup requirements. Add Barracuda Chromebook Security Extension.



App	Installation policy
Allow users to install other apps & extensions	Allow all other apps & ex Locally applied
Google Drive apdfllckaahabafndbhieahigkjlhalf	Force install + pin Locally added
Gmail pjkljhegncpnkpknbcohdijeoejaedia	Force install + pin Locally added
Dropbox for Gmail dpdmhfocilnekecfjgimjdeckachfbec	Force install + pin Locally added
Barracuda Chromebook Security Extension mlbgnlemejoeocmncpolejmdbimkoiol	
Save to Google Drive gmbmikajjgmnabiglmofipeabaddhgne	

5. Upload the **chromebook_config.txt** file you created in **Step 1** above (if you had saved the file with a '.json' extension, change the file extension to '.txt') to the Google Admin console. In the **Users & Browsers** window, in the right navigation window, click the icon to upload the file as shown below. You'll be prompted to select the text file that you created.



App	Installation policy
Allow users to install other apps & extensions	Allow all other apps & exten Locally applied
Google Drive apdfllckaahabafndbhieahigkjlhalf	Force install + pin Locally added
Gmail pjkljhegncpnkpknbcohdijeojaedia	Force install + pin Locally added
Dropbox for Gmail dpdmhfocilnekecfjgimjdeckachfbec	Force install + pin Locally added
Barracuda Chromebook Security Extension mlbgnlemejoeocmncpolejmdbimkoiol	Allow install Locally added

Barracuda Chromebook Security Extension

Allowed hosts

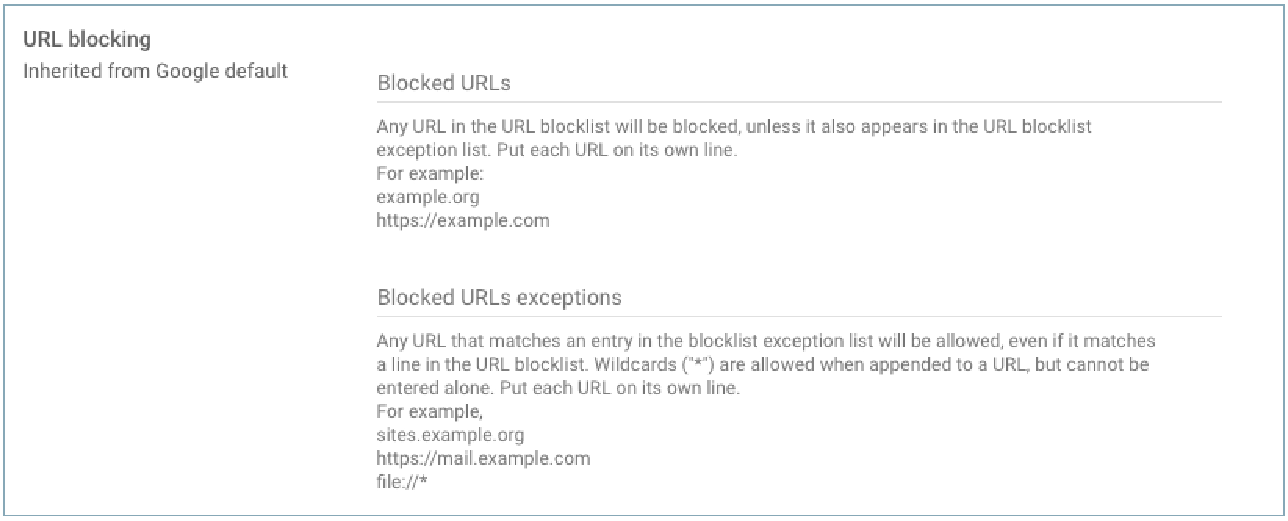
One per line; allowed hosts override blocked hosts

Inherited from Google default

Policy for extensions

```
{
    "webFilterUrl": { "Value":
"10.44.226.44" },
    "webFilterSslPort": { "Value": "443" },
    "sharedKey": { "Value":
"QkByckBjdWRAMTIz" },
    "catServer": {
        "Value":
"api.uswest1.aws.wcs.cudasvc.com"
```

6. Go to **Devices > Chrome > Apps & extensions**. In the **Apps & extensions** drop-down, click **Settings**. Scroll down to the **Content** section and, in the **URL Blocking** section, add these URLs to the **URL Blocklist**:
chrome://policy
chrome://extensions
chrome://indexeddb-internals/



URL blocking
Inherited from Google default

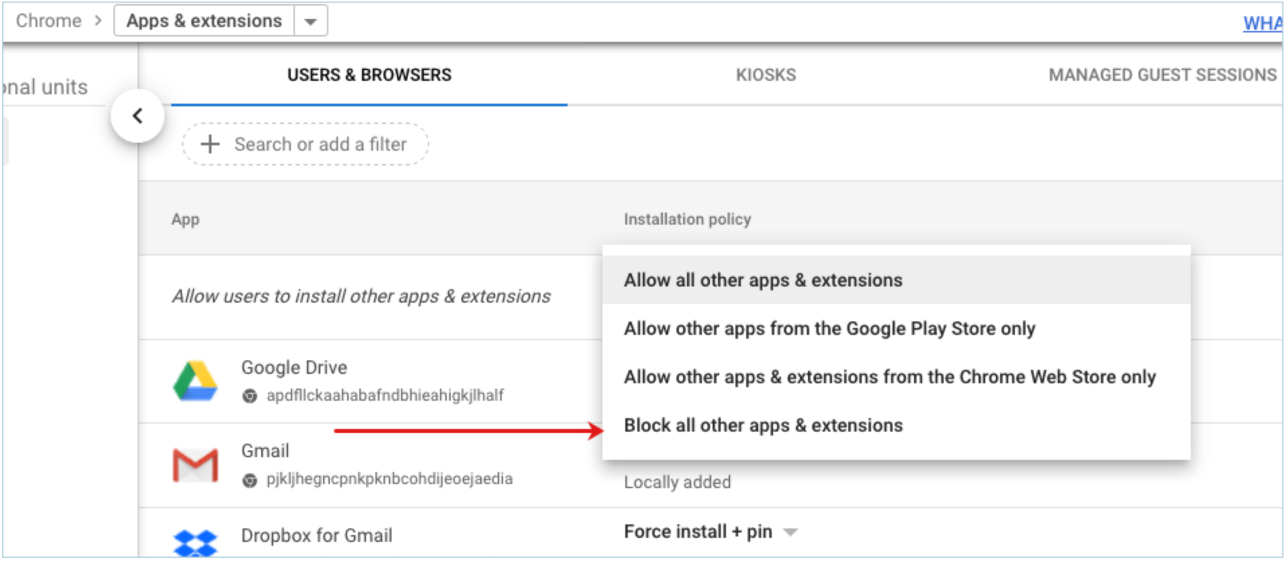
Blocked URLs

Any URL in the URL blocklist will be blocked, unless it also appears in the URL blocklist exception list. Put each URL on its own line.
For example:
example.org
https://example.com

Blocked URLs exceptions

Any URL that matches an entry in the blocklist exception list will be allowed, even if it matches a line in the URL blocklist. Wildcards ("*") are allowed when appended to a URL, but cannot be entered alone. Put each URL on its own line.
For example,
sites.example.org
https://mail.example.com
file://*

7. Click **SAVE** in the upper right of the page.
8. Go to **Devices > Chrome > Users & Browsers**, and select **Apps & extensions** from the drop-down**.** Use the drop-down for **Allow all other apps & extensions** and disable options for the user to install extensions by selecting **Block all other apps & extensions.**



Chrome > Apps & extensions

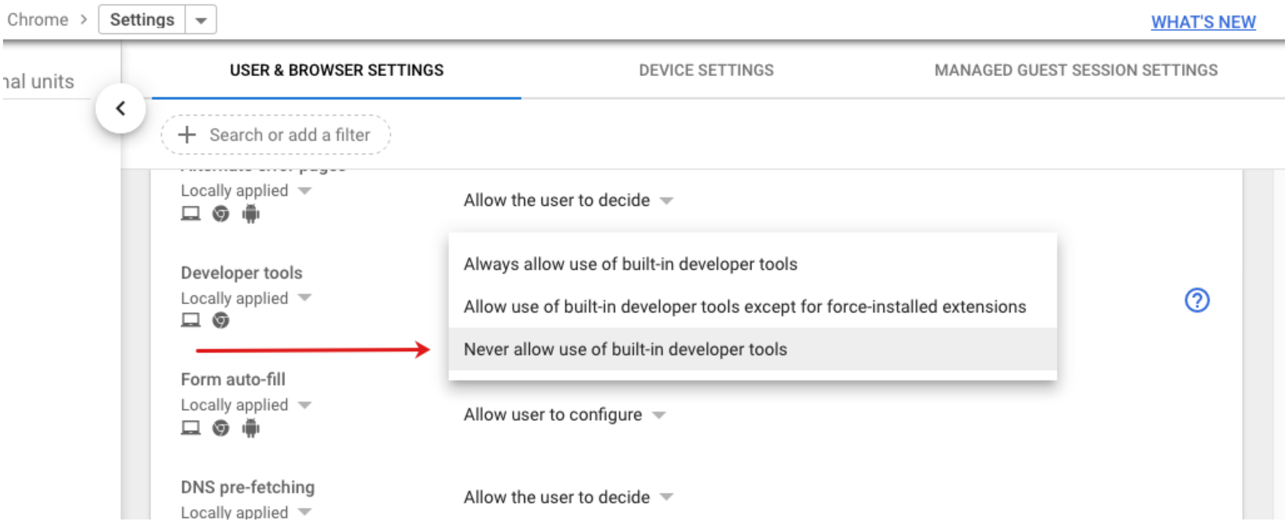
nal units

USERS & BROWSERS | KIOSKS | MANAGED GUEST SESSIONS

Search or add a filter

App	Installation policy
Allow users to install other apps & extensions	Allow all other apps & extensions Allow other apps from the Google Play Store only Allow other apps & extensions from the Chrome Web Store only Block all other apps & extensions
Google Drive apdfllckaahabafndbhieahigkjlhalf	
Gmail pjkljhegncpnkpknbcohdijeoejaedia	Locally added
Dropbox for Gmail	Force install + pin

9. Go to **Devices > Chrome > User & Browser Settings.** Scroll down to the **User Experience** section and, next to **Developer Tools**, use the drop-down to select **Never allow use of built-in developer tools.**



Chrome > Settings

WHAT'S NEW

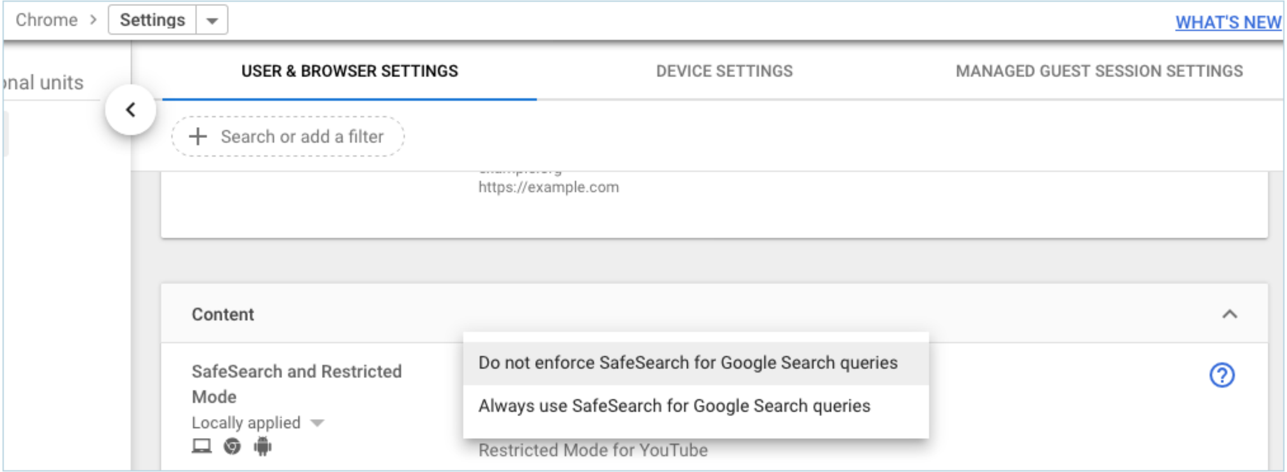
al units

USER & BROWSER SETTINGS | DEVICE SETTINGS | MANAGED GUEST SESSION SETTINGS

Search or add a filter

Locally applied	Allow the user to decide
Developer tools Locally applied	Always allow use of built-in developer tools Allow use of built-in developer tools except for force-installed extensions Never allow use of built-in developer tools
Form auto-fill Locally applied	Allow user to configure
DNS pre-fetching Locally applied	Allow the user to decide

10. Go to **Devices > Chrome > User & Browser Settings** and scroll down to the **Content** section. Next to **Safe Search and Restricted Mode,** enable **Safe Search** by selecting **Always use Safe Search for Google Search queries.**



Chrome > Settings

WHAT'S NEW

USER & BROWSER SETTINGS | DEVICE SETTINGS | MANAGED GUEST SESSION SETTINGS

Search or add a filter

https://example.com

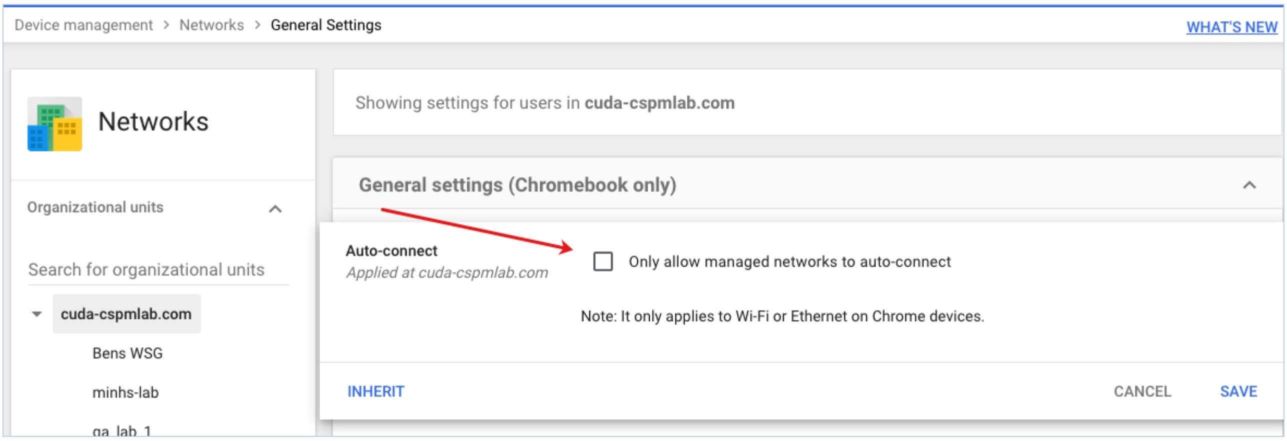
Content

SafeSearch and Restricted Mode
Locally applied

Do not enforce SafeSearch for Google Search queries
Always use SafeSearch for Google Search queries

Restricted Mode for YouTube

11. Go to **Device Management > Network > General Settings** and make sure that **Auto-connect** is *not* checked.



Device management > Networks > General Settings

WHAT'S NEW

Networks

Organizational units

Search for organizational units

cuda-cspmlab.com
Bens WSG
minhs-lab
qa_lab_1

Showing settings for users in **cuda-cspmlab.com**

General settings (Chromebook only)

Auto-connect
Applied at cuda-cspmlab.com

□ Only allow managed networks to auto-connect

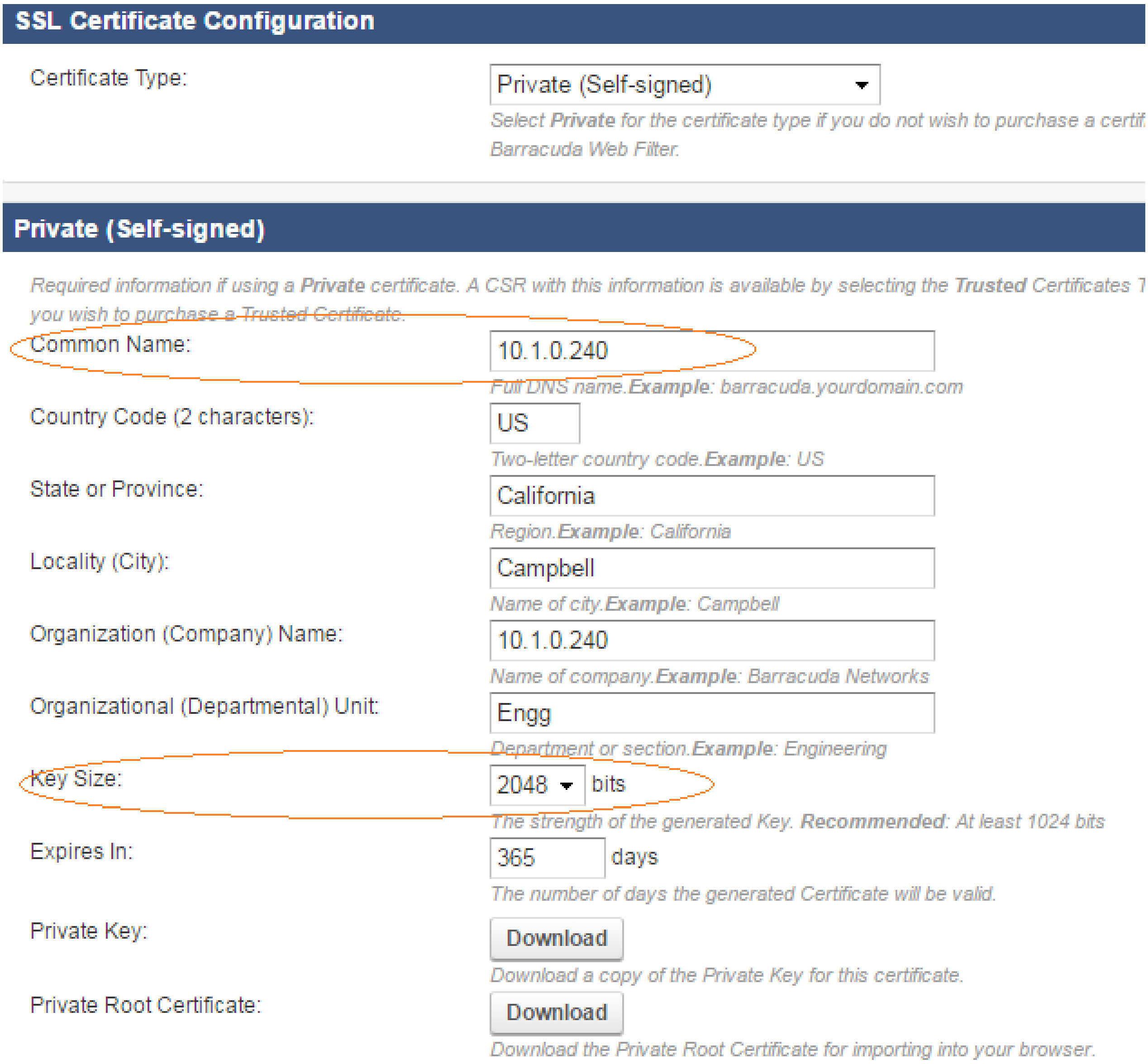
Note: It only applies to Wi-Fi or Ethernet on Chrome devices.

INHERIT | CANCEL | SAVE

Step 3. Configure a Secure Administration certificate on the Barracuda Web Security Gateway.

Important: If you change the date on the Barracuda Web Security Gateway certificate, a new certificate is created and you must redeploy it to the Barracuda Chromebook Security Extension.

1. On the Barracuda Web Security Gateway, go to the **ADVANCED > Secure Administration** page. On this page, you can create or upload an SSL certificate. Click **Help** on that page to read more about using SSL certificates.
2. In the **SSL Certificate Configuration** section, select the **Certificate Type** as **Private(Self-Signed)** and fill in the details with the **Common Name** as the Barracuda Web Security Gateway IP address (or a hostname that resolves to that IP address) , and **Key Size** as **2048**. Click **Save**.



SSL Certificate Configuration

Certificate Type: Private (Self-signed)

*Select **Private** for the certificate type if you do not wish to purchase a certif Barracuda Web Filter.*

Private (Self-signed)

*Required information if using a **Private** certificate. A CSR with this information is available by selecting the **Trusted** Certificates T you wish to purchase a Trusted Certificate.*

Common Name: 10.1.0.240

*Full DNS name. **Example**: barracuda.yourdomain.com*

Country Code (2 characters): US

*Two-letter country code. **Example**: US*

State or Province: California

*Region. **Example**: California*

Locality (City): Campbell

*Name of city. **Example**: Campbell*

Organization (Company) Name: 10.1.0.240

*Name of company. **Example**: Barracuda Networks*

Organizational (Departmental) Unit: Engg

*Department or section. **Example**: Engineering*

Key Size: 2048 bits

*The strength of the generated Key. **Recommended**: At least 1024 bits*

Expires In: 365 days

The number of days the generated Certificate will be valid.

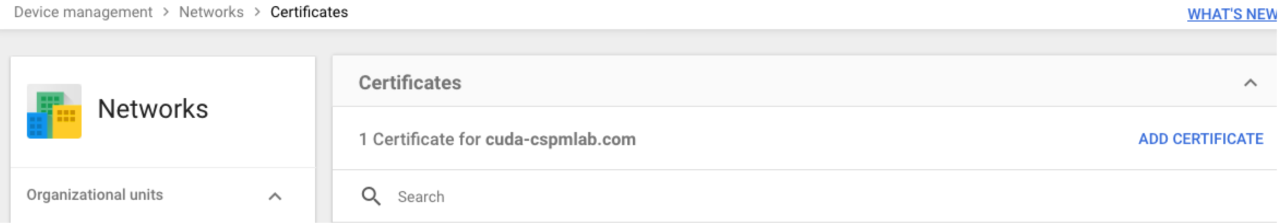
Private Key: Download

Download a copy of the Private Key for this certificate.

Private Root Certificate: Download

Download the Private Root Certificate for importing into your browser.

3. Reload the page, and then download the **Private Root Certificate**.
4. On the Google Admin console, go to **Device Management > Network > Certificates**. Click **Add Certificate** and upload the certificate.



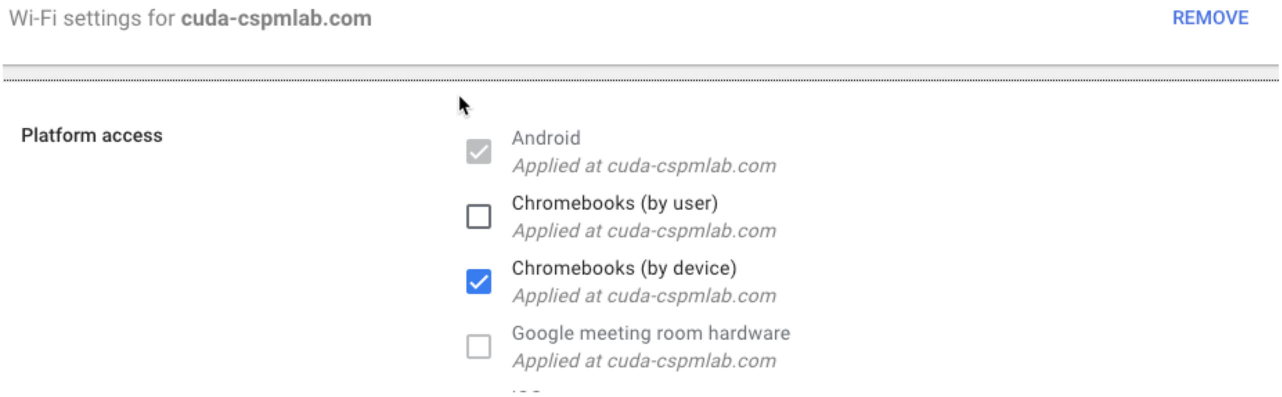
1 Certificate for cuda-cspmlab.com

5. Select **Use this certificate as an HTTPS certificate authority**. Click **Save**.

Step 4. Proxy web traffic to the Barracuda Web Security Gateway

Each SSID that is known to be behind the Barracuda Web Security Gateway that the Barracuda Chromebook Security Extension will connect to needs to be defined in admin.google.com with proxy settings as shown in the following steps. This step prevents inline SSL Inspection Barracuda Web Security Gateway deployments from blocking Chromebooks from authentication with Google on the Chromebook login screen. For proxy deployments or non-SSL Inspection deployments, this step is not necessary, but recommended as it will avoid any deployment related issues in case deployment is switched at some point from proxy deployment to inline.

1. Log into Google Admin console as an administrator and go to **Device Management > Networks > Wi-Fi**. Select the Wi-Fi network to manage.
2. Make sure that, in the **Platform Access** section, **Chromebooks (By Device)** is checked, not **Chromebooks (By User).**



Wi-Fi settings for **cuda-cspmlab.com**

Platform access

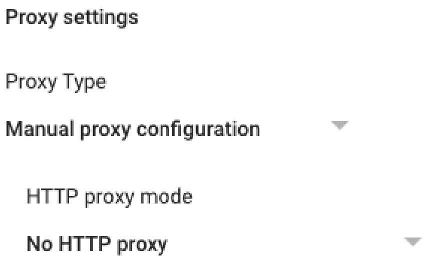
☑ Android
Applied at cuda-cspmlab.com

☐ Chromebooks (by user)
Applied at cuda-cspmlab.com

☑ Chromebooks (by device)
Applied at cuda-cspmlab.com

☐ Google meeting room hardware
Applied at cuda-cspmlab.com

3. Change **Proxy Settings** to **Manual Proxy Configuration**.

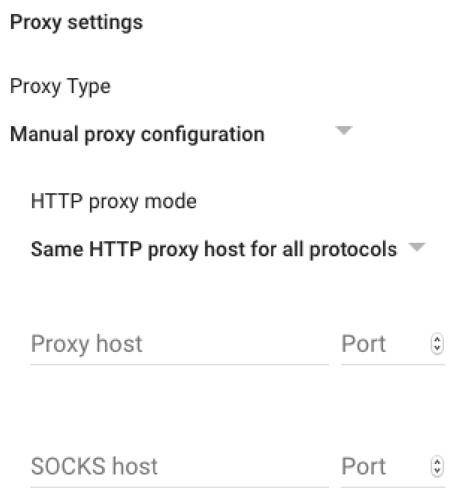


Proxy settings

Proxy Type
Manual proxy configuration

HTTP proxy mode
No HTTP proxy

4. Under **HTTP proxy mode**, select **Same HTTP proxy host for all protocols**.
5. Enter the host IP address or hostname for **Proxy host** and the Proxy Port configured on the **ADVANCED > Proxy** page for the **Port**.



Proxy settings

Proxy Type

Manual proxy configuration

HTTP proxy mode

Same HTTP proxy host for all protocols

6. Click **Save**.

Set Up Single Sign-on for Active Directory (AD) to Sync With Google Accounts

This setup is optional.

1. Download the Google Cloud Directory Sync (GCDS) https://support.google.com/a/answer/6120989?hl=en
2. In the Google Admin console, go to **Domains > Add/remove Domains** and enter your public domain name into your admin.google.com account.
3. Follow instructions at https://support.google.com/a/answer/6123891 to configure GCDS to sync your user configuration for LDAP.
4. Follow instructions at https://support.google.com/a/answer/2611842?hl=en to use Google Workspace Password Sync (GSPS) to sync user passwords with your LDAP.`

When Using SSL Inspection

If you enable the **SSL Inspection** feature on the Barracuda Web Security Gateway (set to **'On'** on the **ADVANCED > SSL Inspection** page), be sure to do the following:

1. Download a client certificate from the **Advanced > SSL Inspection** page.
2. On the Google Admin console, go to **Devices > Network > Certificates**. Click **Add Certificate** and upload the certificate.
3. Select **Use this certificate as an HTTPS certificate authority**. Click **Save**.

Next, add the domains listed by Google: Set Up a Hostname Allow List to the **Exempted Domains** section of the page. This step prevents inline Barracuda Web Security Gateway deployments from blocking Chromebooks from authentication with Google on the Chromebook login screen.

How to Update the Barracuda Chromebook Security Extension

When there is a new version of the extension available, the user must log out of the Chromebook and log in again to get the latest version. Any time the user logs in, the latest version of the extension is in place.

Figures