

Chromebook OS

- [Chromebook Filtering Setup](#)

Chromebook Filtering Setup

How to set up the filtering on Chromebook

Changing DNS in the network settings

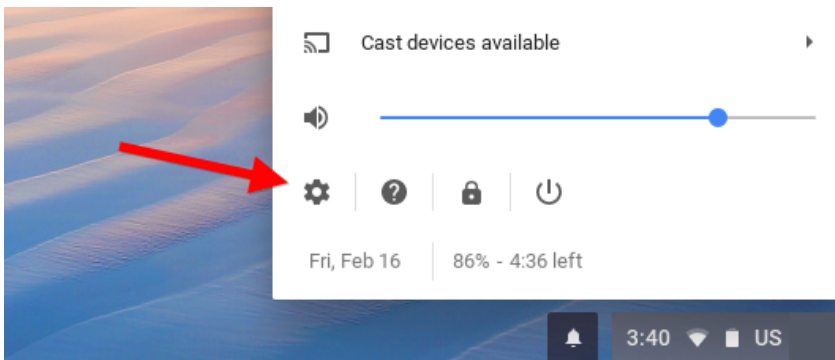
1. Go to SafeDNS **Dashboard > Settings > Devices**, copy your IP address to the "**IP addresses / DynDNS**" box, choose a policy, and click "**Add**".

Your IP address	IPv4 DNS-servers addresses	IPv6 DNS-servers addresses
162.210.194.38	195.46.39.39 195.46.39.40	2001:67c:2778::3939 2001:67c:2778::3940

IP addresses/DynDNS	0/13
---------------------	------

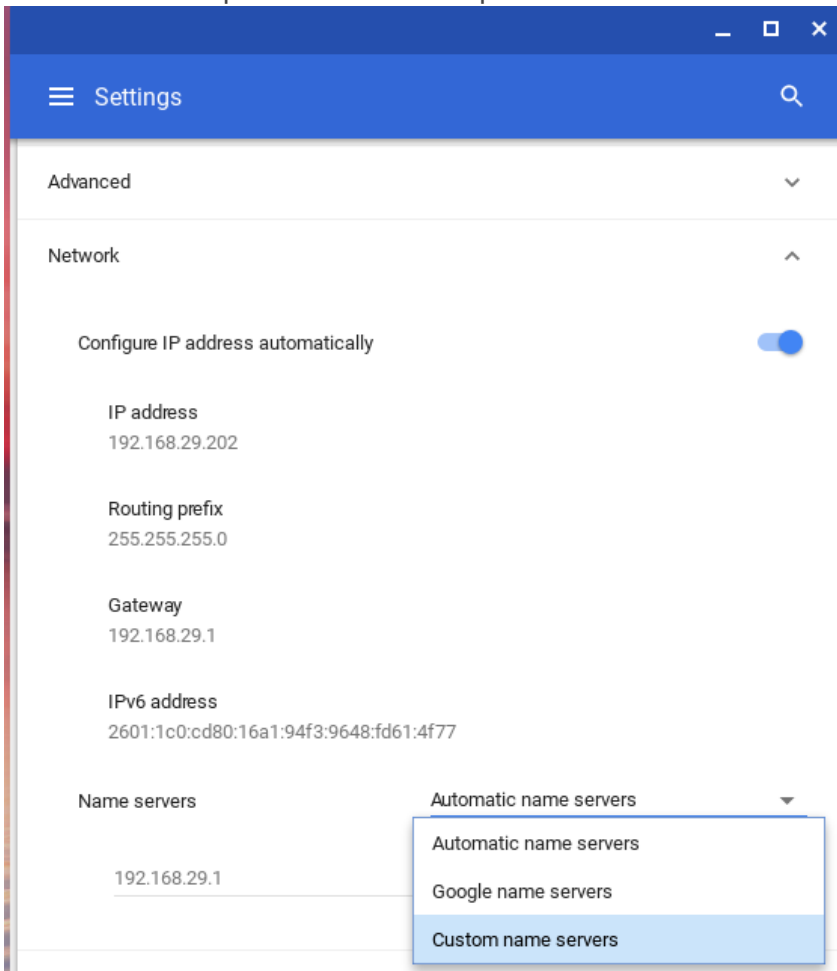
Default Add Edit as List

2. From the Homepage of your Chromebook, click on the menu icon in the top right of the screen and navigate to Settings.
Alternatively, you can click on the notification tray and then press the gear-shaped Settings icon.



3. Navigate to Network and select your connection (Wi-Fi or Ethernet).
4. Click the network name > Network.

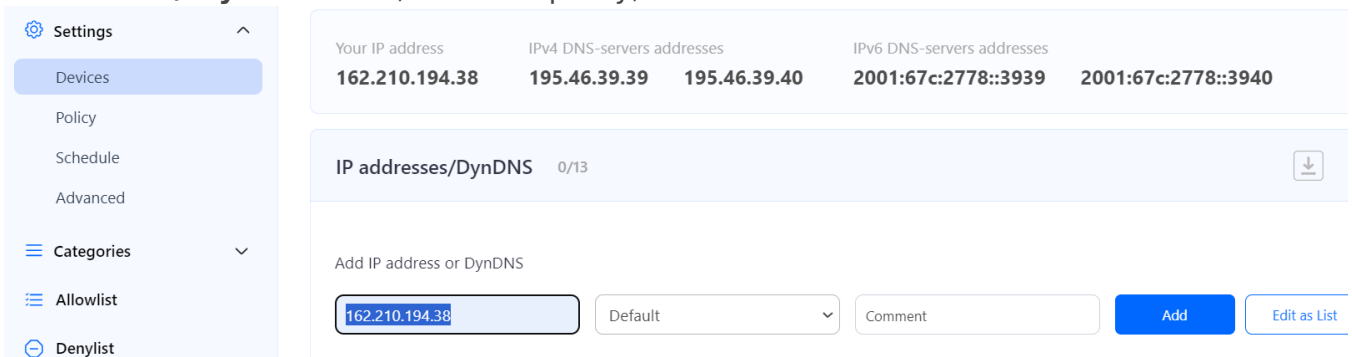
5. In the Network section of your Chromebook settings, scroll down and select the Custom name servers option from the dropdown menu.



6. Enter the addresses of SafeDNS servers in the Custom name servers fields:
195.46.39.39
195.46.39.40

DNS-over-HTTPS (DoH) in Chrome Browser

1. Go to SafeDNS **Dashboard > Settings > Devices**, copy your IP address to the "**IP addresses / DynDNS**" box, choose a policy, and click "**Add**".



2. Open Chrome Browser
3. Select Settings from the dropdown menu after clicking on the three vertical dots (menu) in the upper-right corner of the browser.
Alternatively, enter chrome://settings/security in the URL field, and press Enter. Go to Step

- 6.
4. Click Privacy and Security on the left panel.
5. Click on Security.
6. In the Advanced section of the security settings, you will see an option labeled Use secure DNS.
7. Toggle the switch to On.
8. In the section "Select DNS Provider", click on Add custom DNS provider
9. Paste URL: <https://doh.safedns.com/>

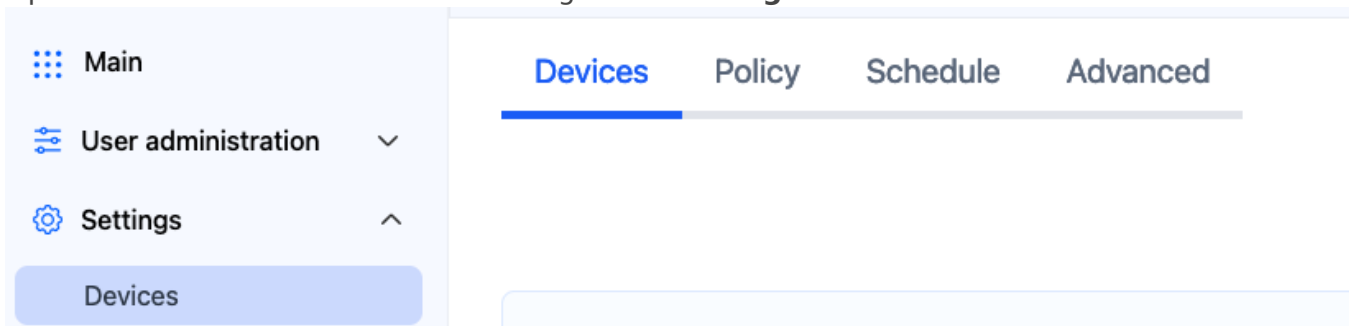
Please note that the **doh.safedns.com** URL works only if your network's IP address is added to the SafeDNS Dashboard.

Pro, Pro Plus, Education & Non-profit plans offer DoH links that work in any network without adding an IP address.

Filtering setup via OpenVPN

This method works on Chromebooks that support Google Play Store apps.

1. Open the SafeDNS Dashboard and navigate to **Settings > Devices**.



2. Scroll down to the VPN section, enter any name for a new VPN connection, and click Add. Choose a filtering policy before adding a VPN connection, if needed.



A screenshot of the 'VPN' section in the SafeDNS Dashboard. At the top, it says 'VPN 0/25'. Below this is a section titled 'Add VPN'. It contains a text input field with 'Home Network' entered, a dropdown menu currently showing 'Default', and a blue 'Add' button. Below the 'Add VPN' section is a search bar with 'VPN' entered and a magnifying glass icon. At the bottom, there is a table header with three columns: 'Name', 'Policy', and 'Certificate'. Under the 'Name' column, it says 'List is empty'.

3. Upon creating the connection, two icons will appear in the "Certificate" column. One is for downloading the Certificate, and the other is for sending it by email. Press the "Cloud download" icon.

Multiple devices can use the same filtering policy, but each device should use its own VPN certificate.

You can also change the filtering policy of the created VPN connection by clicking on the pencil icon to the right. Please note that you don't need to redownload your VPN certificate on your mobile device if you change its filtering policy.

The screenshot shows a VPN management interface. At the top, there's a header "VPN 1/25". Below it, a section "Add VPN" contains a text input "Enter connection name", a dropdown menu set to "Default", and a blue "Add" button. Below this is a search bar with "VPN" entered. The main part of the interface is a table with three columns: "Name", "Policy", and "Certificate". The first row in the table has "Home Network" under Name and "Default" under Policy. In the Certificate column for this row, there are two icons: a cloud with a download arrow and an envelope icon. A red arrow points to the cloud download icon. To the right of the table, there are icons for editing (pencil) and deleting (trash).

Name	Policy	Certificate
Home Network	Default	 

4. Install OpenVPN from the Google Play Store.
5. Launch the app and add the previously downloaded certificate.

How to restrict DNS changes on Chromebook

Administrators can restrict network changes and enforce DNS policies if the Chromebook is enrolled in a Google Workspace account.

Enforcing a DNS server on managed Chromebooks

1. Log in to Google Admin Console.
2. Navigate to **Devices > Chrome > Settings > Users & Browsers**.
3. Scroll to Network settings and disable the "**Allow user to configure network**" option.
This prevents users from modifying DNS settings.
4. Set Enforced DNS servers to **195.46.39.39** and **195.46.39.40**
5. Save and apply changes.

Policies automatically sync to enrolled Chromebooks.

Enforcing DoH (DNS-over-HTTPS) on managed Chromebooks

Configuring DoH can be done locally in a browser, and can be managed via your Google Workspace Admin.

1. Log in to Google Admin Console.
2. Navigate to **Devices > Chrome > Settings > Users & Browsers**.
3. Navigate to the DNS-over-HTTPS option.
4. Select "**Enable DNS-over-HTTPS without insecure fallback**", and enter the DoH URL - **doh.safedns.com**.
5. Save and apply changes.

This will make the Secure DNS option in Chrome disabled for users.

Please note that the **doh.safedns.com** URL works only if your network's IP address is added to the SafeDNS Dashboard.

Pro, Pro Plus, Education & Non-profit plans offer DoH links that work in any network without adding an IP address.

Unmanaged Chromebooks

Without management tools, direct control over local DNS settings is not possible. However, you can enforce DNS restrictions indirectly.

- Set up the filtering on the [router level](#). All connected devices will be filtered automatically.
- If supported by the router, redirect or block unauthorized DNS traffic on ports 53 and 853.