NetSpective WebFilter Extension for Chrome

GROM
EDUCATIONAL SERVICES

Printed in the United States of America

Grom Educational Services, Inc.
3280 Pointe Parkway, Suite 2500
Peachtree Corners, GA 30092
www.gromedu.com

Table of Contents

The NetSpective WebFilter Extension for Chrome

The NetSpective WebFilter Extension for Chrome was designed to filter Chromebooks both on or off campus. This suits the most common Chromebook deployments which are one-to-one initiatives, and on campus deployments where multiple users may use a single Chromebook.

NetSpective WebFilter Extension for Chrome filters browser traffic without the use of a proxy server.

Unlike the NetSpective Remote Agent for Windows and macOS, the Extension runs inside the Web Browser and will enforce policy on traffic before SSL encryption. However, it does not filter traffic from the ChromeOS Services and Chrome Apps such as locally installed games.

As of 5.3.0, the Chrome Extension fails OPEN in the event it cannot communicate with the NetSpective.

Prerequisites

There are several steps that should be performed before deploying Extension for Chrome. Please review the following:

1. The Chrome Extension requires a fully licensed and updated NetSpective appliance.

2. Assign a hostname to NetSpective in your DNS servers, e.g., webfilter.example.com. Google requires a valid Internet hostname so don't use .local domains.

3. If you are planning to filter your Chromebook off campus. It will be necessary to configure your Firewall Rules for inbound traffic to the NetSpective appliance on TCP port 8443. The DNS name for your appliance must be accessible from both inside and outside of your network.

4. Install an SSL Certificate on the appliance. The certificate cannot be a self-signed certificate. It must be signed by a public Certificate Authority (CA) or recognized as a valid CA by all of the devices in your network and Chromebooks.

5. Verify that NetSpective has the correct time. In the Device Settings > Advanced > System Time section, set the local time zone, and then press *Test NTP Server* to assure your appliance has

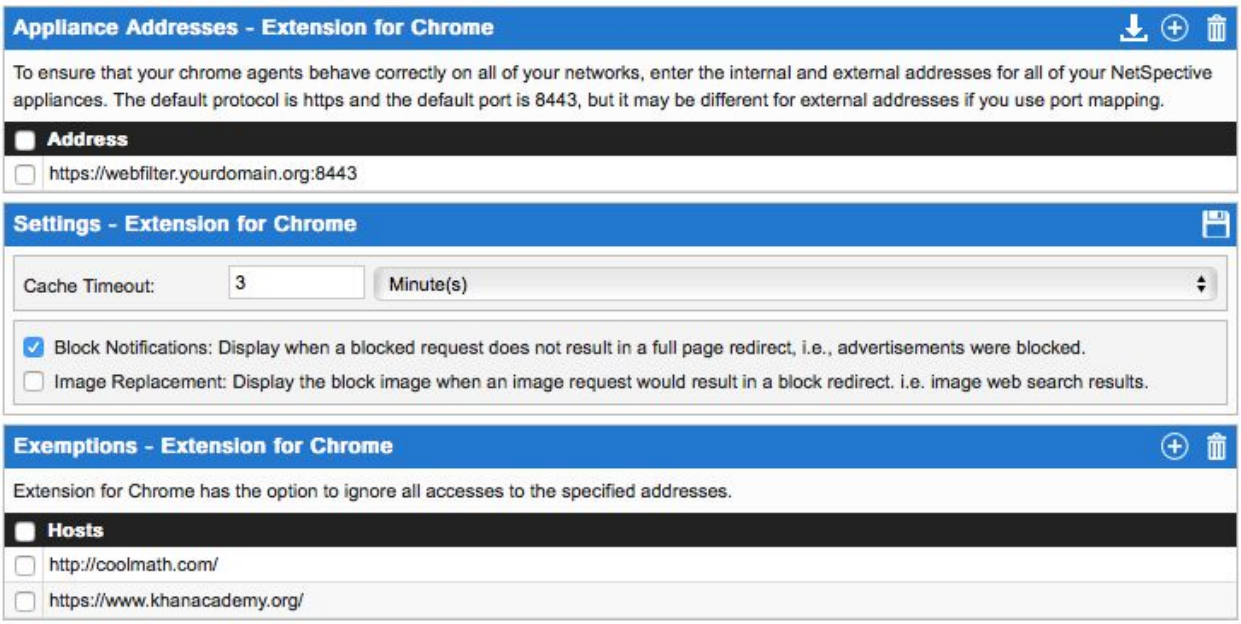
connectivity to a timeserver. A valid test will display "NTP Server Test OK." If you do not receive this message, consider changing the server IP address to a local NTP server or check your firewall rules.

6. You must have access to the Google Admin Console, https://admin.google.com, for your domain.

7. The Google's consoles work best with the Chrome web browser. You may download and install the Chrome web browser from https://www.google.com/chrome/browser/desktop/index.html.

Preparing for the Deployment

In the NetSpective Web Administration, navigate to Authentication > Extension for Chrome



Appliance Addresses – Extension for Chrome, select the Add button on the far right to add the Internal and External addresses of all your NetSpective appliances, one address at a time. Normally in the format of https://webfilter.example.com:8443. The hostname of the appliance(s) must match the SSL certificate installed on each appliance and have corresponding DNS entries.

Settings – Extension for Chrome, configure the behavior of the Chrome Extension. The Cache Timeout reduces communication between the Chrome Extension and the NetSpective by caching the last known policy for the user. The extension can then perform blocks and allows without asking the NetSpective for a policy check for each access. The default setting is 3 minutes, and we recommend opening a discussion with NetSpective Support before changing this value.

Notifications for Blocks – If you are surfing web content and parts of a webpage are being blocked, but the full page is not being blocked, the Chrome Extension can display a notification. This notification simply tells you a block occurred and the corresponding category.

Image Replacement – If images on a page are being blocked and filtered, checking this option will replace the blocked image with the NetSpective block icon.

Exceptions – Extension for Chrome, you can add URLs for websites that are allowed here. These exceptions will not be processed by the Chrome Extension and will go through the browser untouched.

When you are finished, click the download button at the top right and save the **appliances.json** file. This file will be used when Deploying the Chrome Agent.

Note: Each time you choose to add or edit these settings, you must download this file, and then update Google Admin Console.

Deploying the Extension for Chrome

The Chrome Extension like any other Chrome app can automatically installed (or force-install) on all of your Chromebooks through the Google Admin Console. Through this method, users will not be able to remove the extension from their account. If you would like additional information, please visit Google's support article for automatically installing apps.

https://support.google.com/chrome/a/answer/6306504?hl=en

Setup

Before you can force-install apps or extensions for your users, you need to turn on their **Chrome Web Store** service in your Admin console. You can find this service in your Admin console by going to **Apps** > **Additional Google Services**. For detailed steps, see Turn Additional Google Services on or off.

Force-install the Extension for Chrome

1. Sign into the Google Admin console at https://admin.google.com/.

2. From the Admin console dashboard, click **Device Management**.

3. On the left, click **Chrome management**.

4. Click **App management**.

5. In the Find or Update Apps section, cut and paste the App ID shown below into the search field, and then press the Search button.

   ID: plojahkfikogcanoonlnbdajiljjhpid

6. Select the category of settings you want to configure:
   User settings: Force-install the item for users who sign in with an account in your domain.

Public session settings: Force-install the item for users who sign in to a public session on your devices.

7. In the **Orgs** section on the left, click the organizational unit where you want to force-install the item. To install items for everyone your organization, select the top-level organizational unit.

8. Under **Force Installation**, click  to turn the setting on  .
Note: If you're force-installing an item for a child organization, the force install setting might be inherited from the top-level organization. Click **Override** to change the setting from it's parent. For more information, see How the organizational structure works.

9. Under **Configure**, select **UPLOAD CONFIGURATION FILE.** Navigate to the appliances.json file you downloaded in the previous section.

10. Click **Save**.

Force-installing an app or extension gives it permission to access information on the device it's installed on.

Disable Incognito Mode and Developer Tools

To avoid user tampering with the operation of the Extension for Chrome, please disable Incognito Mode and Developer Tools options on the Chromebooks.

1. Sign in to the Google Admin console at https://admin.google.com/.

2. From the Admin console dashboard, click **Device Management**.

3. Under **DEVICE SETTINGS**, click **Chrome Management.**

4. Click **User Settings**.

5. Select the proper OU for your users.

6. Under the **Security** heading, locate the **Incognito Mode** option and then select **Disallow**.

7. Under the **User Experience**, locate **Developer Tools** option and then select **Never allow the use of built-in developer tools**.

8. Click **Save**.