SonicWall™ Content Filtering
Client 3.1
Agent Guide
SonicWall™ offers comprehensive web content security that blocks selected web content and enforces protection and productivity policies. The main components are Content Filtering Service (CFS), Content Filtering Client (CFC), and EPRS (Enforced Policy & Reporting System). CFS protects the devices behind the firewall; CFC protects devices regardless of where the device is located, even if it is connected outside the firewall, and EPRS provides administrators with the means to manage CFC from a central web interface.

This document describes how to use SonicWall Content Filtering Client interface on the user systems. You can view basic status including policy information such as active policy name, last successful policy update, and last report sent. In addition, you can view the status for override, if allowed by the policy, and license details such as the serial number, expiration and version. This guide describes the different user interface views and actions that can be taken with each.

For this release, the Content Filtering Client interface has been simplified for easier use and unified to work with Windows, Mac OS and Chrome clients.

Topics:
- Policy
- Settings
- Forbidden Items
- SonicWall Support
Policy

The Policy page of the interface shows both policy and licence status.

Topics:

- Policy Section
- Active Policy
- Licence Section

Policy Section

In the Policy section, each field listed is an active link. When you run the cursor over it, it becomes bold and italics to indicate that you can select it.

The fields in the Policy view are defined below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Policy</td>
<td>When selected expands to show the status of the current active policies. Refer to Active Policy for more information. Click on Active Policy again to hide the policy status.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Requests an update to the policies from EPRS. If the update is successful, the current date and time changes to reflect the update time.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If an update is not successful then the date and timestamp does not change. You can open the logs to see the error that is preventing the update.</td>
</tr>
<tr>
<td>Last Report Sent</td>
<td>Sends the latest reports to the EPRS. If the update is successful, the current date and time changes to reflect the time the report was sent to EPRS.</td>
</tr>
</tbody>
</table>
Active Policy

When selected, the Active Policy field is an active link that expands to show the status of the default policies. Click on Active Policy again to hide the policy status.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter HTTP</td>
<td>Off/On</td>
<td>When On, filters the HTTP sites the user tries to access.</td>
</tr>
<tr>
<td>Filter HTTPS</td>
<td>Off/On</td>
<td>When On, filters the HTTPS sites the user tries to access.</td>
</tr>
<tr>
<td>Safe Search</td>
<td>Off/On</td>
<td>When On, enables Safe Search policies for Google and Bing.</td>
</tr>
<tr>
<td>Suspend behind FW</td>
<td>Off/On</td>
<td>When On, suspends the on-board content filtering client and allows the network security appliance to filter web content when the end user system is in the office and behind firewall.</td>
</tr>
</tbody>
</table>

![Content Filtering Client Interface]

SonicWall Content Filtering Client 3.1 Agent Guide
Content Filtering Client
**Licence Section**

In the License section, each field is informational rather than an active link.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Displays the serial number of the firewall or the Client Distribution Group associated with your configuration.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Lists when the CFC license expires.</td>
</tr>
</tbody>
</table>

![License Section Table](image)

**Settings**

The Settings page groups diagnostics and support information. The Windows and Mac OS Settings are the same, but a Chrome system has additional options.

**Topics: :**

- Windows and Mac OS Settings
- Chrome OS Settings

**Windows and Mac OS Settings**

The Settings window for Windows and Mac OS systems show the options View Logs, Send TSR, and Run Diagnostics.

![Windows and Mac OS Settings](image)
Viewing Logs

Under Settings, click on View Logs and the CFC log file opens in another window. The log file keeps a record of the different types of events generated by CFC and the date and time they occurred. Four types of messages are tracked:

- Info
- Warning
- Error
- Debug

Sending a TRS

Under the Support section, you can opt to Send TSR. A TSR is a Tech Support Report. When you click on Send TRS, a diagnostic report is sent to the support team at SonicWall. The Content Filtering Client also displays a message requesting that you contact SonicWall Support and gives you the host name of your system, which you need to get support. See the screen capture below for an example of the message.

Running Diagnostics

If you choose Run Diagnostics, CFC runs a diagnostic check and generates a report that opens a browser. The report includes the following information:

- Checking installation
- Checking configuration
- Checking license server
- Checking policy server
- Checking botnet server
- Checking WebRDS server
- Checking WebCFS server
- Checking TSR uploads server
- Checking reporting server
You can use the diagnostic report to pinpoint where possible issues lie. A segment of that diagnostics report is shown as an example below:

<table>
<thead>
<tr>
<th>Checking installation</th>
<th>Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking install location</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking for install directory</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking for service binary</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking for dashboard binary</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking for driver binary</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking for CA certificates</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking if Content Filtering Client service is installed</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking if Content Filtering Client service is running</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking if Content Filtering Driver service is installed</td>
<td>Pass</td>
</tr>
<tr>
<td>Checking if Content Filtering Driver service is running</td>
<td>Fail</td>
</tr>
</tbody>
</table>

### Chrome OS Settings

The Settings window for Chrome OS systems show the options for **Settings** and **Support**.

![Chrome OS Settings Window](image)

- **Settings**:
  - Debug Logging
  - Clear Logs
  - View Logs

- **Support**:
  - Email Logs
  - Send TSR
  - Run Diagnostics
Chrome OS Settings Options

The Settings section of the page has several options for a Chrome system.

<table>
<thead>
<tr>
<th>Settings Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug Logging</td>
<td>Debug logging can be enabled or disabled on the end user system. When the button is to the left with the background gray, as shown in the figure above, logging is disabled. Slide the button to the right to enable debug logging and the background turns blue.</td>
</tr>
<tr>
<td>Clear Logs</td>
<td>Clears the Content Filtering Logs. You are asked to confirm that you want to clear the logs since it can’t be undone.</td>
</tr>
<tr>
<td>View Logs</td>
<td>Displays the Content Filtering Logs. A sample excerpt of the log file is shown below.</td>
</tr>
</tbody>
</table>

![Content Filtering Logs](image)

---

**Sample Log File:**

```
2016-10-19 09:28:57.638 Passing policy message to extension
2016-10-19 09:28:57.683 Policy received from EPRS has not changed.
2016-10-19 09:28:57.683 Policy information parsed, result = 8
2016-10-19 09:28:57.804 CF[8] Active filter changed to 'Copy of Default'
2016-10-19 09:28:57.712 CF[8] update finished, result is 0
2016-10-19 09:28:57.714 Chrome storage changed in area 'local'
2016-10-19 09:28:57.715 Chrome storage changed in area 'local'
2016-10-19 09:28:57.720 CF[8] Saving policy to disk
2016-10-19 09:28:57.792 CF[8] License and policy servers will be checked again Tue Dec 2016-10-19 09:28:57.793 Chrome storage changed in area 'local'
2016-10-19 09:28:57.795 Chrome storage changed in area 'local'
2016-10-19 09:30:05.339 Opening View Logs...
2016-10-19 09:30:06.348 Opening View Logs...
2016-10-19 09:30:06.511 View Logs window opened.
2016-10-19 09:30:06.622 Log View opened...
2016-10-19 09:30:08.670 CF[8] Checking domain to ip map for 'mail.google.com'
2016-10-19 09:30:08.678 CF[8] ip for 'mail.google.com' is '216.58.194.197'
2016-10-19 09:30:12.547 CF[8] Checking domain to ip map for 'docs.google.com'
2016-10-19 09:36:51.585 CF[8] ip for 'docs.google.com' is '173.194.283.189'
```
Chrome OS Support Options

Under the Support section, you can opt to Email Logs, Send TSR, or Run Diagnostics.

<table>
<thead>
<tr>
<th>Support Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Logs</td>
<td>If you need support you can opt to send an email to your local administrator. When you click on Email Logs, a zip file is created from the Content Filtering logs and an email template with system information is opened for you (see below). Input the email address of the recipient, attach the file tsr.zip from the Downloads file, and send the email.</td>
</tr>
</tbody>
</table>

```
SonicWALL Content Filtering Client for Chrome OS Version 3.1.24.124
OS: Chrome OS
OS Version: 53.0.2785.154
OS Platform: x86_64
Device ID: 3E191F3C-E01D-10A4-C542-F127E7CAD519

Note: You Must Attach the Downloaded file TSR.zip that was saved in the Downloads folder. You can also drag and drop the TSR.zip file from the Downloads folder into this email
```

| Send TSR         | A TSR is a Tech Support Report. When you click on Send TRS, a diagnostic report is sent to the support team at SonicWall. Content Filtering Client also displays a message requesting that you contact SonicWall Inc. support and asks you to mention our login ID when calling. |

```
The TSR was successfully received. Please contact SonicWall support at www.sonicwall.com/support and mention your login email 'fumarro@gedu.demo.sonicwall.com'
```

<table>
<thead>
<tr>
<th>Run Diagnostics</th>
<th>If you choose Run Diagnostics, CFC runs a diagnostic check and generates a report that opens a browser. The report includes the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Checking configuration</td>
</tr>
<tr>
<td></td>
<td>• Checking license server</td>
</tr>
<tr>
<td></td>
<td>• Checking policy server</td>
</tr>
<tr>
<td></td>
<td>• Checking botnet server</td>
</tr>
<tr>
<td></td>
<td>• Checking WebRDS server</td>
</tr>
<tr>
<td></td>
<td>• Checking WebCFS server</td>
</tr>
<tr>
<td></td>
<td>• Checking TSR uploads server</td>
</tr>
<tr>
<td></td>
<td>• Checking reporting server</td>
</tr>
</tbody>
</table>
Forbidden Items

The Forbidden Items page allows you to view the Categories, Domains, Keywords, Botnets, and Other items that were blocked due to policy configuration. It shows the blocked event counters for each item. The example below shows three blocked events due to Categories match. No details are available.

NOTE: The Botnet option is not shown on Chrome OS systems.

About

The About page displays the copyright and warranty information about the SonicWall Content Filtering Client. The screen capture below shows a portion of this text. This is also where you can find the version number of Content Filtering Client if you need it for support purposes.
SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

To view the SonicWall End User Product Agreement (EUPA), see https://www.sonicwall.com/legal/eupa.aspx. Select the language based on your geographic location to see the EUPA that applies to your region.