



SonicWall™ Content Filtering Client 3.1.56

Release Notes

June 2017

These release notes provide information about SonicWall Content Filtering Client 3.1.56 release.

Topics:

- [SonicWall™ Content Filtering Client 3.1.56](#)
- [Supported Platforms](#)
- [Resolved Issues](#)
- [Product Licensing](#)
- [SonicWall Support](#)

About Content Filtering Client 3.1.56

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

The Content Filtering Client service provides protection and productivity policy enforcement for businesses, schools, libraries, and government agencies. Policies are configured by the administrator and then applied to clients based on user and group membership. The service blocks objectionable and unproductive web content even when the client machine is outside the firewall perimeter. Client machines automatically receive the latest software updates for filtering web content.

The Content Filtering Client 3.1.56 release resolves some issues from the previous release. Refer to [Resolved Issues](#) for more information.

Supported Platforms

SonicWall Content Filtering Client 3.1.56 is supported on Windows and Mac OS. The specific operating systems and hardware requirements are noted below:

System Type	OS Level	Hardware
Windows	Windows 10	Processor: 2 Ghz or higher (for both 32-bit and 64-bit)
NOTE: Supports both 32-bit and 64-bit versions.	Windows 8.1	Memory: 2 GB RAM or higher
	Windows 8	
	Windows 7	
Mac OS	10.9 and above	N/A

Resolved Issues

This section provides a list of resolved issues in this release.

CFC on Windows only

Resolved issue	Issue ID
Windows system crashes after Content Filtering Client is installed.	184952
Occurs when Content Filtering Client is installed on Windows 10 Pro/Enterprise.	

CFC on Windows and Mac

Resolved issue	Issue ID
Content Filtering Client does not automatically trim trailing spaces/new-line characters from the hash.	182161
Occurs after upgrading to the latest version. Client must trim leading or trailing spaces or new-line character from the hashes so that hashes match correctly.	
Content Filtering Client continues to filter internet access based on previous policy.	185075
Occurs when a specific policy was previously defined and then the Default and Scheduled policies are set to None from the Enforcement policy in the EPRS.	
Content Filtering Client stops filtering Botnet IPs.	185152
Occurs when the filtering is first suspended behind a firewall and then moved to another network where it is re-enabled. When Content Filtering is restarted, Botnet filtering resumes normal functioning.	

Product Licensing


SonicWall Content Filtering Client can be licensed by:

- [Licensing in MySonicWall](#)
- [Licensing from a Network Appliance](#)

Licensing in MySonicWall

To license in MySonicWall:

- 1 Log into MySonicWall.
- 2 Select the link in the **Free Trial Software** section.
- 3 Under **Anti-Virus/Content Filter Client**, type a descriptive name into the **Friendly Name** field and click **Try Now**.
- 4 On the **Manage Client Distribution Group Services** page, scroll down to the **Applicable Services** section.
- 5 In the row for Content Filtering Client, click either the **Try, Buy, or Activate** button to license the CF Client.

 **NOTE:** To activate the license you need to have the license code from a previous purchase of the service.

Licensing from a Network Appliance

To license from a network appliance:

- 1 Log into your network security appliance as administrator.
- 2 Navigate to the **System > Licenses** page.
- 3 Under **Manage Security Services Online**, select the link **To Activate, Upgrade, or Renew services, click here**.
- 4 Enter your MySonicWall credentials to log in and open the Service Management page.
- 5 Scroll down to the **Applicable Services** section and locate the Content Filtering Client service.
- 6 Click either the **Try, Buy, or Activate** link to license the Content Filtering Client.

When complete, your firewall displays the updated license status on the **System > Status** page.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support 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 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, visit <https://support.sonicwall.com/contact-support>.

Copyright © 2017 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal/>.

Legend



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 6/15/17

232-003939-00 Rev A