SonicOS 6.2.6 Content Filtering Service (CFS) 4.0

Feature Guide

August 2016

This feature guide describes the SonicOS 6.2.6 Content Filtering Service (CFS) release 4.0. CFS 4.0 delivers content filtering enforcement for educational institutions, businesses, libraries and government agencies. These organizations can control the websites students and employees can access using their IT-issued computers, while behind the organization's firewall.

Topics:

CFS 4.0 Overview

CFS 4.0 compares requested websites against a massive cloud database that contains millions of rated URIs, IP addresses and websites. It also provide administrators with the tools to create and apply policies that allow or deny access to sites based on individual or group identity or by time of day. CFS 4.0 has been redesigned to improve performance and ease of use.

To achieve this goal, duplicate code was removed, and the CFS framework and workflow was redesigned. In prior versions, features were fragmented across categories, but they have now been consolidated under the CFS category to enable central management. More accurate filtering options have been provided, and the code has been improved to handle small packets. For more information on how to upgrade from CFS 3.0, refer to *SonicOS 6.2.6 Content Filtering Service (CFS) 4.0 Upgrade Guide*.

When processing packets, CFS 4.0 follows this workflow:

1. A packet arrives and is examined by CFS.
2. CFS checks it against the configured exclusion addresses and allows it through if a match is found.
3. CFS checks its policies and finds the first policy which matches the following conditions in the packet:
    - Source zone
    - Destination zone
    - Address object
    - Users/group

- Schedule
- Enabled state

4 CFS uses the CFS Profile Object defined in the matching policy to do the filtering and returns the corresponding action for this packet.

5 CFS performs the action defined by the CFS Action Object in the matching policy.

6 If no policy is matched, the packet is passed through without any action by CFS.

CFS 4.0 Features

The new features and enhancements for CFS 4.0 include the following:

- CFS settings (which includes global settings, exclusions, custom category settings, and advanced settings)
- CFS Custom Categories
- CFS policy design
- URI List Objects
  - Importing and exporting URI List Objects
  - Matching URI List Objects (including wildcard matching)
  - Using CFS URI List Objects
- Action objects
  - CFS Passphrase
  - CFS Confirm
  - CFS bandwidth management
- Profile objects
- CFS logs

CFS settings

CFS 4.0 makes use of numerous settings that help define filtering parameters. Most are set on the Content Filter page, but the Advanced Settings are nested within the CFS Policies when you create a new profile. Table 1 defines the settings and lists where in the tool they can be found.

Table 1. Settings for CFS 4.0

Type and Location	Setting	Definition
Global Settings		
Security Services > Content Filter; go to section called **Global Settings**	Max URL Caches (entries)	Defines the maximum number of cached URL entries. Cached URL entries save the URL rating results, so that SonicOS does not need to ask the backend server for the rating of a known URL. In CFS 3.0, the cache was a size specification; in CFS 4.0 it is changed to the maximum number of entries.
	Enable Content Filtering Service	By default, enables content filtering for all packets. Uncheck this option to bypass content filtering for all packets.
	Enable HTTPS content filtering	When enabled, attempts to get the ServerName from the client “hello”. If that fails, CFS attempts to get the CommonName from the SSL certificate and then get the rating. If both attempts fail to get the ServerName or CommonName, CFS uses the IP address to look up the rating.
	Blocked if CFS Server is Unavailable	Defines whether to allow or deny this request if the CFS server cannot provide the rating request within the specified period. The system default is 5 seconds. You may enter a different value in the **Server Timeout** field.
CFS Exclusions		
Security Services > Content Filter; go to the section called **CFS Exclusions**	Exclude Administrator	When enabled, bypasses content filtering for all requests from an account with administrator privileges.
	Excluded address	Bypasses content filtering for all requests from address objects selected in the **Excluded address** list.
CFS Custom Category		
Security Services > Content Filter; go to the section called **CFS Custom Category**	Enable CFS Custom Category	Allows you to customize the categories for specific URLs. When CFS checks the ratings for a URL, it first checks the user ratings and then checks the CFS backend server for the ratings. Up to 10,000 custom category entries are supported. Refer to CFS Custom Categories for details on how to define custom categories for a domain.
Advanced Settings		
Security Services > Content Filter; go to the section called **CFS Policies** and select **Add...> Create New Profile > Advanced.**	Enable Smart Filtering for Embedded URL	When enabled, detects the embedded URL inside Google Translate (https://translate.google.com) and filters the embedded URL too. Requires that client DPI-SSL be enabled also.
	Enable Safe Search Enforcement	Enforces Safe Search when searching on any of the following websites: • www.yahoo.com • www.ask.com • www.dogpile.com • www.lycos.com Requires that client DPI-SSL be enabled also if the website is using HTTPS.

Table 1. Settings for CFS 4.0

Type and Location	Setting	Definition
	Enable Google Force Safe Search	When enabled, overrides the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action. Note that typically Safe Search happens automatically and is powered by Google, but when this options is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address. **NOTE:** This feature only takes affect only after DNS of client host has been refreshed.
	Enable YouTube Restrict Mode	When enabled, accesses YouTube in Safety mode. YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals. **NOTE:** This feature only takes affect only after DNS of client host has been refreshed.
	Enable Bing Force Safe Search	When enabled, overrides the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action. **NOTE:** This feature only takes affect only after DNS of client host has been refreshed.

CFS Custom Categories

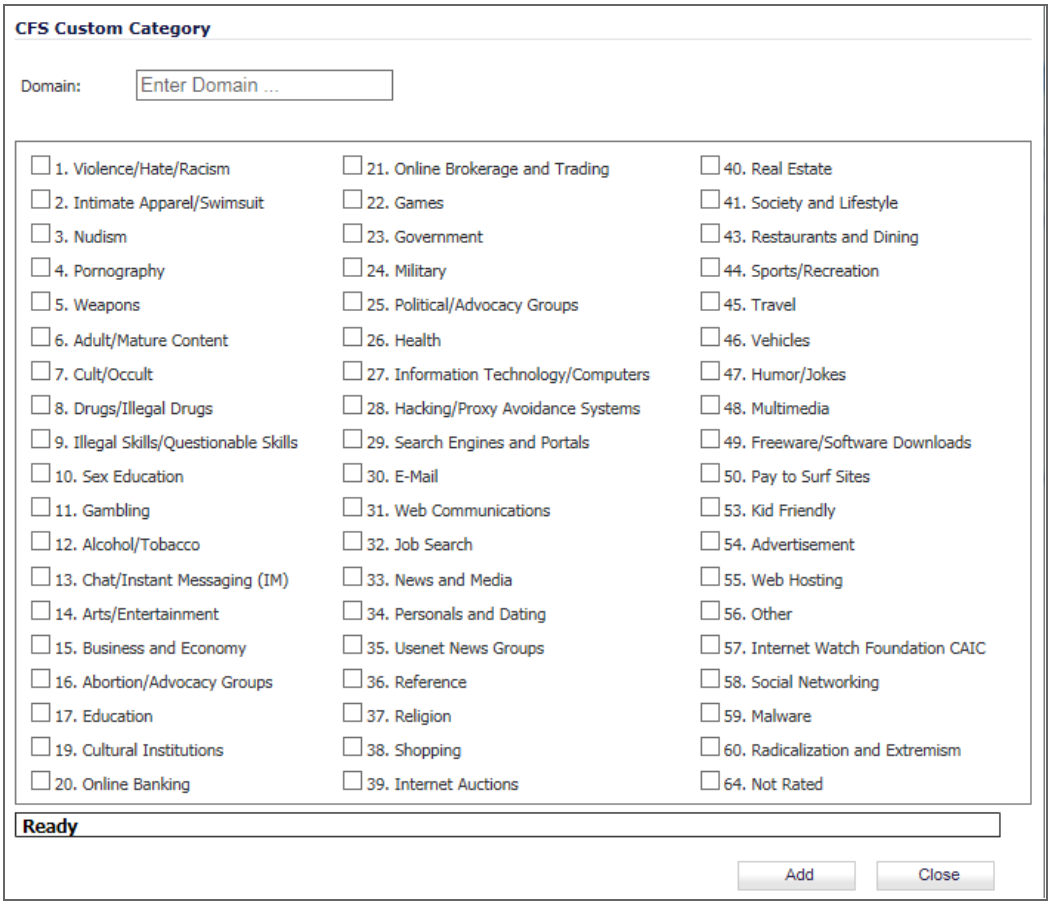
You can customize ratings for certain domains, and up to 10,000 valid entries are supported. When CFS checks the ratings for one URI, it checks the user rating first and then checks the rating from the backend server. Custom categories are processes like those categories provided by the backend server.

To define a custom category:

1 Navigate to **Security Services > Content Filter** and find the **CFS Custom Category** heading.

2 Be sure the **Enable CFS Custom Category** check box is selected.

3 Select **Add...**.



4 Input a valid URI in the Domain field.

5 Select up to four categories to assign to that URI.

6 Select **Add**. The domains having a customized category definition are listed in the Custom Category table.

Additional options are provided for managing the Custom Category list:

- Delete a custom category by checking the box beside the domain name and select **Delete**.
- **Export** and **Import** functions are supported. The best practice is:
  a Select a set of domains and export them to a file.
  b Use that file as a template and update the information.
  c Import the new file. The files should reflect the following format:

  `<Domain Name>: <Rating1>[,<Rating2>[,<Rating3>[,<Rating4>]]]`

  Entries should be separated by a carriage return or line separator. The following separators are supported:

Separator	Style
`\n`	UNIX style, new line separator
`\r\n`	Windows style, new line separator
`\r`	MAC OS style, new line separator

- A search function is supported so you can more easily search for a specific domain in a long list. Enter the search string in the field called **Lookup Domain Containing String**.
- All custom categories can be deleted by selecting all entries and clicking on **Delete All**.

NOTE: If you believe that a web site is rated incorrectly or you wish to submit a new URI, go to this web site to submit your request: http://cfssupport.sonicwall.com/Support/web/eng/newui/viewRating.jsp.

CFS policy design

A CFS 4.0 policy defines the filtering conditions that a packet is compared to. A default policy is provided, but you can define your own. When writing your own policies, the following parameters can be defined:

- Name
- Source Zone
- Destination Zone
- Source Address
- User/Group
- Schedule
- Profile
- Action

If a packet matches all these conditions, the packet is then filtered according to the corresponding CFS Profile, and the CFS Action is applied. Refer to Action objects and Profile objects for more information.

NOTE: If authentication data for User/Group is not available during matching, no match is made for this condition. This strategy prevents performance issues, especially when Single Sign-On is in use.

Each CFS policy has a priority level, and policies with higher priorities are checked first.

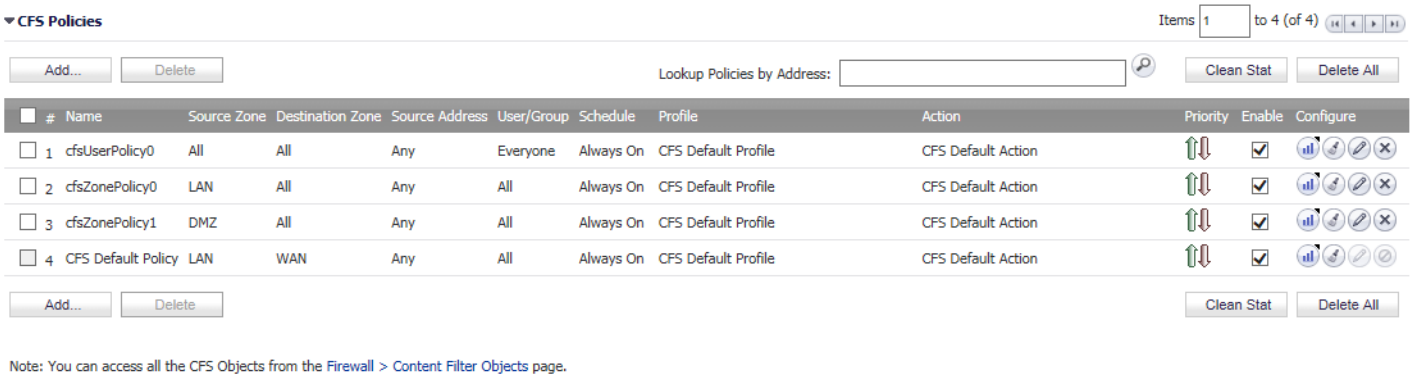
CFS uses a policy table internally to manage all the configured policies. For each policy element, the table is constructed by the configuration data and runtime data. The configuration data includes parameters that are used to define the policy from the user interface, such as policy name, properties and others. The runtime data includes the parameters that are used for packet handling.

CFS also uses a policy lookup table to accelerate runtime policy lookup. Currently, this lookup table contains three dimensions as matching conditions; they are source zone, destination zone, and Address Object (ipv4 AO or ipv6 AO).

Adding a new policy

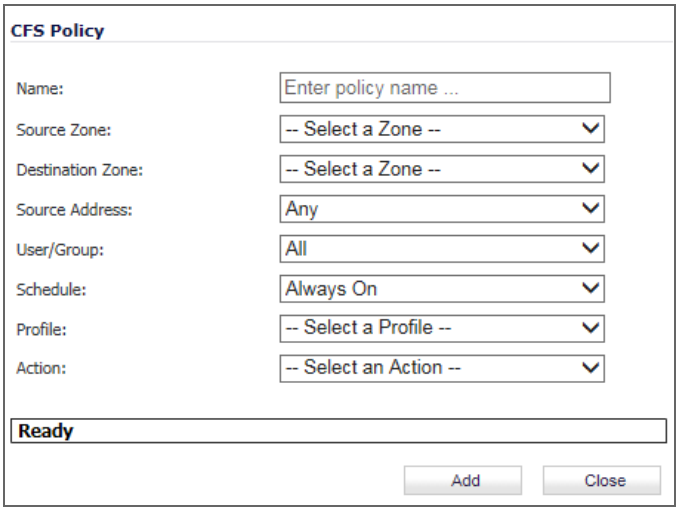
To add a new CFS policy:

1 Navigate to **Security Services > Content Filter** and find the **CFS Policies** heading.



2 Select **Add...**.

3 On the CFS Policy page, enter the policy name in the **Name** field.



4 Select the **Source Zone** from the list provided.

5 Select the **Destination Zone** from the list provided.

6 Select a **Source Address** by choosing **Create new Address**, **Any**, an option from **Address Groups** or an option from **Address Objects**.

7 Select the **User/Group** to apply the policy to. The default is **All**.

8 Set the **Schedule** for the policy. Choose from the options provided or **Create a New Schedule**.

9 Select a **Profile**. Choose from the options provided or choose **Create a New Profile**. Refer to Profile objects for more information about how to create a new profile.

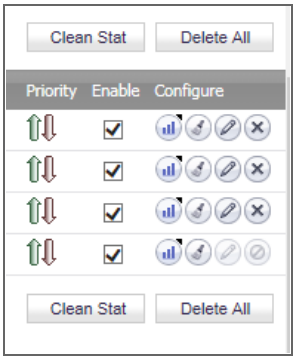
10 Select an **Action**. Choose from the options provided or choose **Create a New Action**. Refer to Action objects for more information about how to create a new Action.

11 Select **Add** when complete.

Managing existing policies

Additional options are providing for managing the CFS Policies list:

- Delete a policy by checking the box beside the policy name and select **Delete**.
- A search function is supported so you can more easily find a specific policy in a long list. Enter an IP address in the field called **Lookup Policies by Address** and select the search button. Both IPv4 and IPv6 formats are supported for IP addresses.
- Choose the **Clean Stat** button if you want to clean the statistics for all policies.
- All policies, except the CFS Default Policy, can be deleted by selecting all entries and clicking on **Delete All**.
- In the Policies table, you can move the mouse over some fields and the definitions pop up.
    - If the Source Address is not defined as **Any**, hold the cursor over the Source Address name to see the address properties.
    - Hold the cursor over the Profile field to see the configuration and settings for that policy.
- Individual policies can be managed using the icons on the right side of the priority table (shown in the following figure).



- Priority of the policy can be changed: click the up/down arrow icon and set a specified priority in the popup window. The highest priority is **1**; assigning **0** automatically changes that policy to the lowest priority.
- Check the box to enable using this policy.
- Select the **Statistics** icon to see Policy Statistics. You can see the Hit Count on that policy if you hold your cursor over that icon.
- Select the **Clean** icon if you want to clean the statistics for this entry only.
- Select the **Edit** icon to edit the policy.
- Select the **Delete** icon if you want to delete the entry.

NOTE: The CFS Default Policy cannot be edited or deleted.

You can access all CFS objects by clicking the link under the policy table or navigate to the **Firewall > Content Filter Objects** page.

URI List Objects

The URI list object defines the list of URIs or domains that can be marked as *allowed* or *forbidden*. This is a replacement for the custom lists in prior versions of CFS. You can add, edit, or delete a URI List Object. You can also export the list to an external file and import a file into another list. These objects are configured on the **Firewall > Content Filter Objects** page in the SonicOS management interface.

NOTE: When processing, URI lists have a higher priority than the category of a URI.

The following conditions apply when building a URI List Object:

- A maximum of 128 CFS URI List Objects are allowed.
- In each object, up to 5,000 URIs are supported.
- By definition, a URI is a string containing host and path. Port and other content are currently not supported.
- An IPv4 or IPv6 address string is supported as the host portion of a URI.
- The maximum length of each URI is 255 characters.
- The maximum length of all URs in a List Object is 131,072 characters (1024*128), including one character for each new line (carriage return) between the URIs.
- Each URI can contain up to 16 tokens. A token in a URI is a string composed of the characters:

```
0 through 9
a through z
A through Z
$ - _ + ! ' ( ) ,
```

- The maximum length of each token is 64 characters including one character for each separator (. or /) surrounding the token.
- An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens.

Examples of valid URIs	Examples of invalid URIs
• news.example.com • news.example.com/path • news.example.com/path/abc.txt • news.*.com/*.txt • 10.10.10.10 • 10.10.10.10/path • [2001:2002::2003]/path • [2001:2002::2003:*:2004]/path/*.txt	Using the wildcard character (*) incorrectly can result in invalid URIs such as: • example*.com • exa*ple.com • example.*.*.com **Note:** The wildcard character represents a sequence of one or more tokens, not one or more characters.

Importing and exporting URI List Objects

You can import a file containing a list of URIs. The file can be created manually or can be a file that was previously exported from the appliance. URIs in the file can be separated by any of the following separators:

Separator	Style
\n	UNIX style, new line separator
\r\n	Windows style, new line separator
\r	MAC OS style, new line separator

Only the first 5,000 valid URIs in the file are imported. Invalid URIs are skipped and do not count toward the maximum of 5,000 URIs per URI List Object.

Matching URI List Objects

The matching process for CFS URI List Objects is based on tokens. A valid token sequence is composed of one or more tokens, joined by a specific character, like “.” or “/”. A URI represents a token sequence. For example, the URI `www.example.com` is a token sequence consisting of “www”, “example” and “com”, joined by a “.”. Generally, if a URI contains one of the URIs in a CFS URI list object, then the list object matches that URI.

Normal matching

If a list object contains a URI such as “example.com”, then that object matches URIs defined as:

```
[<token sequence>(.|/)]example.com[(.|/)<token sequence>]
```

For example, the URI List Object matches any of the following URIs:

- example.com
- www.example.com
- example.com.uk
- www.example.com.uk
- example.com/path

The URI List Object does not match the URI:

- specialexample.com

This is because *specialexample* is identified as a different token than *example*.

Wildcard matching

Wildcard matching is supported. An asterisk (*) is used as the wildcard character, and represents a valid sequence of tokens. If a list object contains a URI such as `example.*.com`, then that list object matches URIs defined as:

```
[<token sequence>(.|/)]example.<token sequence>.com[(.|/)<token sequence>]
```

For example, the URI List Object matches any of the following URIs:

- example.exam1.com
- example.exam1.exam2.com
- www.example.exam1.com/path

The URI List Object does not match the URI:

- example.com

This is because the wildcard character (*) represents a valid token sequence that isn't present in *example.com*.

IPv6 Address Matching

IPv6 address string matching is also supported. While an IPv4 address can be handled as a normal token sequence, an IPv6 address string needs to be handled specially. If a list object contains a URI such as "[2001:2002::2008]", then that list object matches URIs defined as:

```
[2001:2002::2008][/<token sequence>]
```

For example, the URI list object matches any of the following URIs:

- [2001:2002::2008]
- [2001:2002::2008]/path
- [2001:2002::2008]/path/abc.txt

IPv6 Wildcard Matching

Wildcard matching in the IPv6 address string is supported. If a list object contains a URI such as "[2001:2002:*:2008]/*/abc.mp3", then that list object matches URIs defined as:

```
[2001:2002:<token sequence>:2008]/<token sequence>/abc.mp3
```

For example, the URI list object matches any of the following URIs:

- [2001:2002:2003::2007:2008]/path/abc.txt
- [2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt

Using CFS URI List Objects

Currently, CFS URI List Objects can be used in three fields:

- Forbidden URI list of a CFS profile
- Allowed URI list of a CFS profile
- Web Excluded Domains of Websense

CFS URI List Objects are used in these fields differently. When used in a Forbidden or Allowed URI list of a CFS profile, the CFS URI List Object acts normally. For example, if the URI List Object contains a URI such as "example.com/path/abc.txt", then that list object matches URIs defined as:

```
[<token sequence>(.|/)] example.com/path/abc.txt[(.|/)<token sequence>]
```

When used by the Web Excluded Domains of Websense, only the host portion of the URI takes effect. For example, if the URI list object contains the same URI as above then that list object matches all domains containing the token sequence *example.com*. The path portion in the URI is ignored.

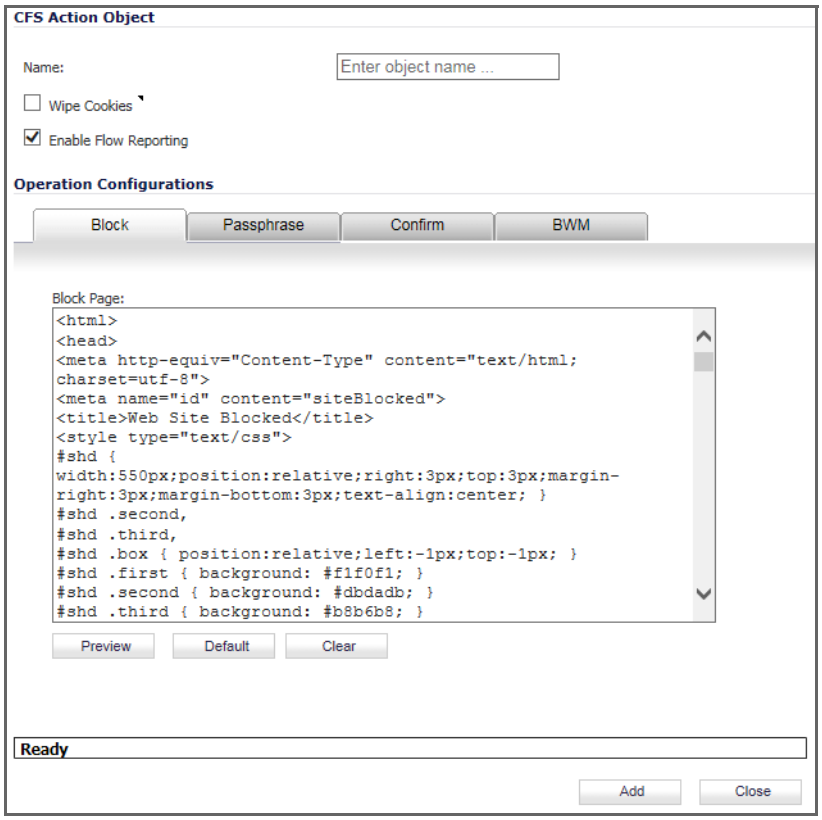
Action objects

The CFS Action Object defines what happens after a packet is filtered by CFS and specified in the CFS Policy.

To define the CFS Action Objects:

1 Navigate to **Firewall > Content Filter Objects**.

2 Find the **CFS Action Objects** heading, and select the **Add...** button in that section.



3 Type the name of the new object in the **Name** field.

4 Choose whether to enable **Wipe Cookies**. If enabled, it removes the cookies inside the HTTP request to protect privacy.

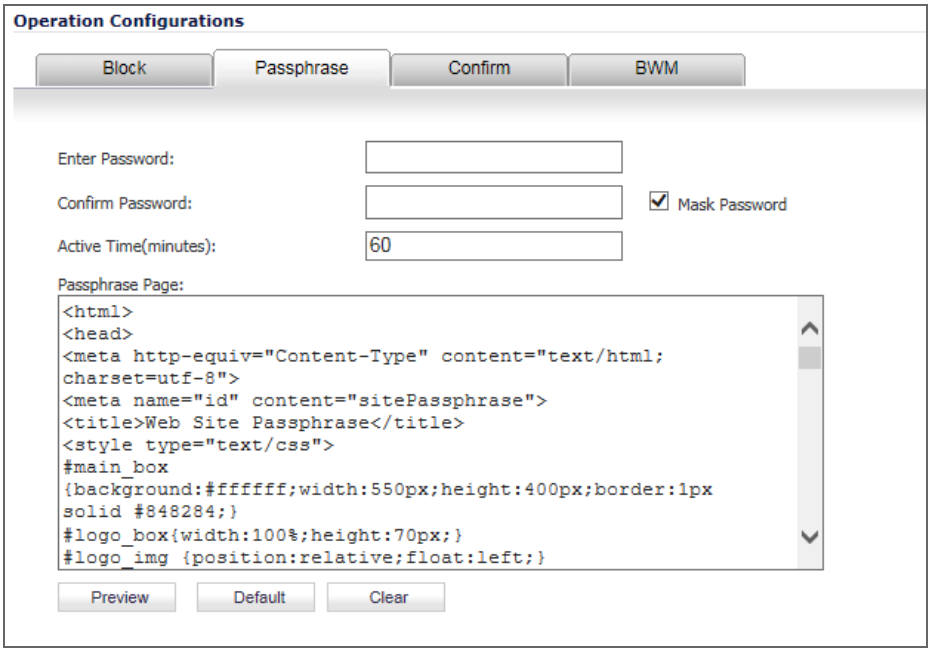
> **IMPORTANT:** If Wipe Cookies is enabled, the Safe Search Enforcement function for some search engines may break.

5 Choose whether to **Enable Flow Reporting**. Checking the box enables the reporting.

6 Select the Block tab to define the block page that displays. A default page is pre-defined, but you can customize it or define your own page.

- Select the **Preview** button to see a preview of the page that has been defined.
- Select the **Default** button to restore the default provided by SonicWALL.
- Select the **Clear** button to clear the page currently defined.

7 Select the **Passphrase** tab to define the parameters for a web page that is password protected. For more information on the Passphrase feature, refer to CFS Passphrase.



a **Enter** the **Password** to access the website.

b **Confirm** the **Password** for the site.

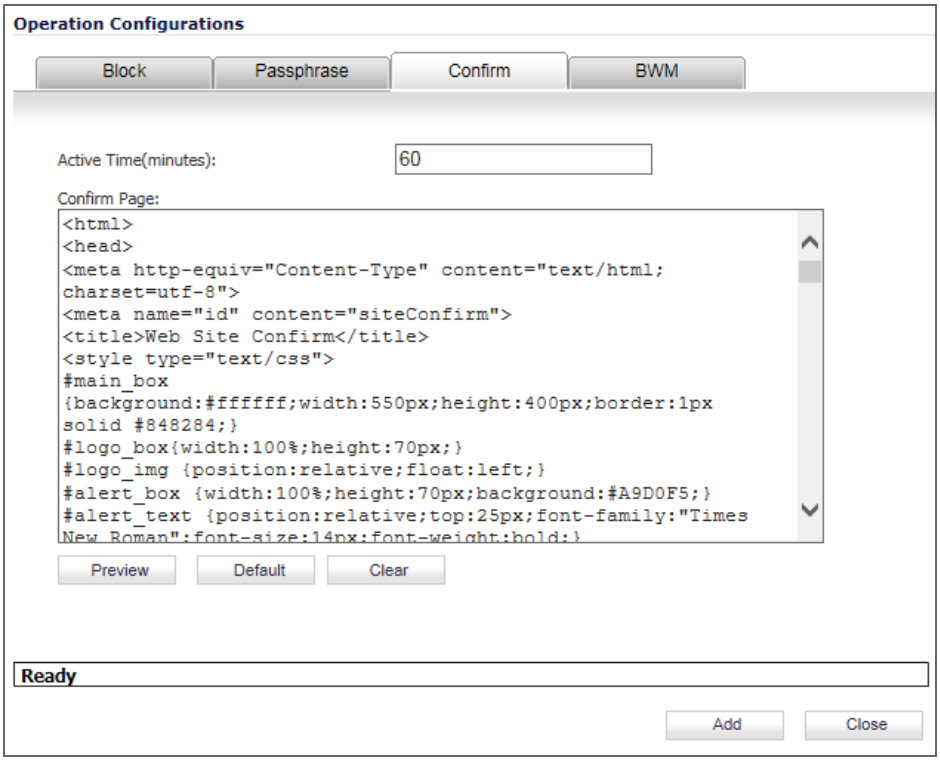
c Check the box if you want to **Mask** the **Password**.

d Enter the **Active Time** (in minutes), or the amount of time that the password is active. The default is 60 minutes, but it can range from 1 to 9999 minutes.

e Set up the **Passphrase Page** that is displayed when a website is password protected. A default page is predefined, but you can customize it or define your own page.

- Select the **Preview** button to see a preview of the page that has been defined.
- Select the **Default** button to set the page to restore the default provided by SonicWALL.
- Select the **Clear** button to clear the page currently defined.

8 Select the **Confirm** tab to define the parameters for a web page that shows a warning or advisory but allows the end user to access it after accepting the Confirm page. For more information on the Confirm feature, refer to CFS Confirm.



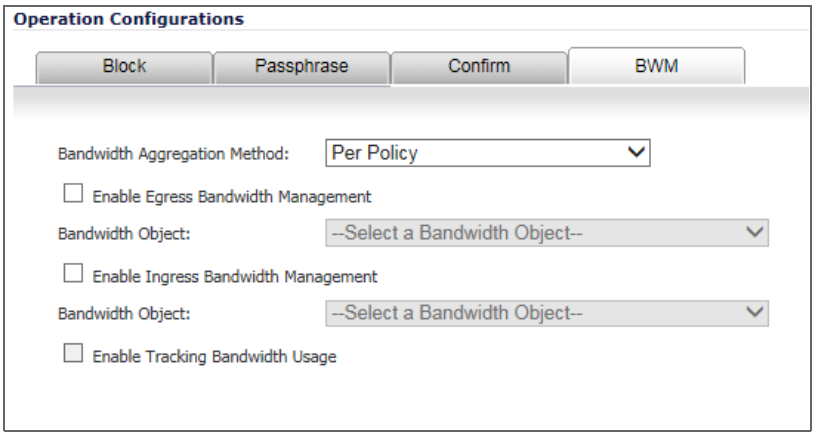
a Enter the **Active Time** (in minutes), or the amount of time that the password is active. The default is 60 minutes, but it can range from 1 to 9999 minutes.

b Setup the **Confirm Page** that is displayed when a website is password protected. A default page is pre-defined, but you can customize it or define your own page.

- Select the **Preview** button to see a preview of the page that has been defined.
- Select the **Default** button to set the page to restore the default provided by SonicWALL.
- Select the **Clear** button to clear the page currently defined.

9 Select the **BWM** tab to set up the bandwidth management parameters. For more information on how to create a bandwidth option for this feature, refer to CFS bandwidth management

IMPORTANT: CFS only supports Bandwidth Management if the BWM type is defined as **Advanced** on the **Firewall Settings > BWM** page in SonicOS.



a Set the **Bandwidth Aggregation Method**. Choose either **Per Policy** or **Per Action**.

b Check the box to **Enable Egress Bandwidth Management**.

c If Egress Bandwidth Management is enabled, set the **Bandwidth Object** for egress, and choose an option for the drop-down menu or create a new Bandwidth Object. Refer to CFS bandwidth management for more information on how to create a new Bandwidth Object.

d Check the box to **Enable Ingress Bandwidth Management**.

e If Ingress Bandwidth Management is enabled, set the **Bandwidth Object** for ingress and choose an option for the drop-down menu or create a new Bandwidth Object.

f Check the box to **Enable Tracking Bandwidth Usage**.

> **NOTE:** Either Egress or Ingress Bandwidth Management, or both, must be enabled to before you can Enable Tracking Bandwidth Usage.

10 Select **Add** when all parameters have been defined.

CFS Passphrase

The passphrase feature is designed to restrict web access based on a passphrase or password. The firewall administrator needs to configure the Passphrase operation for special URI categories or domains (for Forbidden URI List). If users want to access the forbidden URIs, they have to submit the correct password or web access is blocked.

> **IMPORTANT:** Passphrase only works for HTTP requests. HTTPS requests cannot be redirected to a Passphrase page.

The Passphrase operation works in this manner:

1 The user attempts to access a restricted website.

2 A Passphrase page is sent to the user's browser.

3 The user must enter the password and submit it.

4 CFS validates the submitted password with the website's password.

- If the passwords match, web access is allowed. No further passwords are needed, and users can continue to access websites of the same category for the Active Time period that is set for the Passphrase feature. The default is 60 minutes.
- If the passwords don't match, access is blocked and a Block page is sent to the user.

  > **NOTE:** Users have three chances to enter the password. The site is blocked if all chances fail.

- If the user selects Cancel, the site is blocked immediately.

CFS Confirm

The Confirm feature is designed to show an advisory or warning, but requires a confirmation from the user before allowing access. The firewall administrator needs to configure the Confirm operation for special URI categories or domains, and the users need to confirm the web request when they first visit them.

> **IMPORTANT:** Confirm only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page.

The Confirm operation flows in this manner:

1 The user attempts to access a blocked website.

2 A popup appears, requesting confirmation.

3 Users must select **Continue** or **Close**.

- If a user confirms that he wants to access this category of websites, he is redirected to the first confirmed website. No further confirmations are needed, and the user can continue to access

websites of the same category for the Active Time period that is set for the Confirm feature. The default is 60 minutes. The maximum is 9999 minutes.

- If a user chooses Close, he is shown the Block page message and is blocked from that category of website for the period of the Active Time setting.

CFS bandwidth management

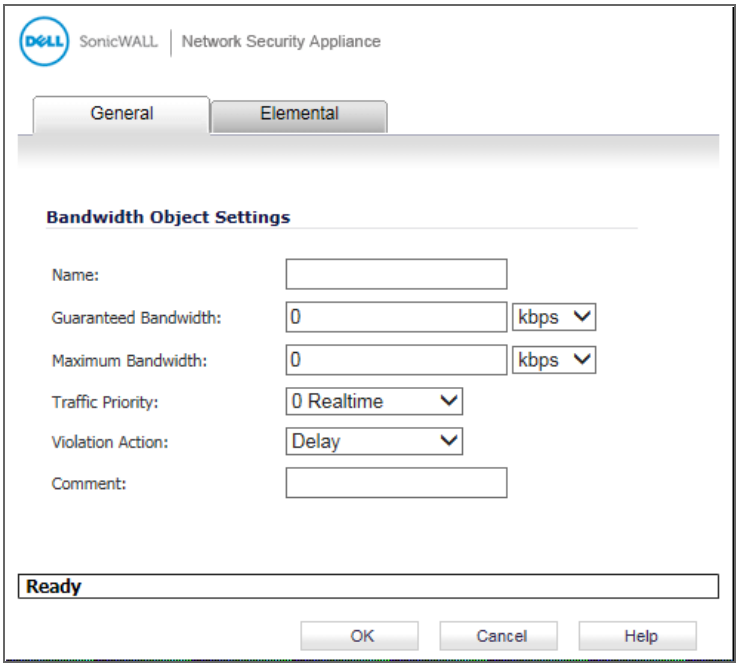
A Bandwidth Object is a feature used within the Action Object to specify how to manage bandwidth for egress and ingress.

To define a Bandwidth Object for CFS:

1 Navigate to the **CFS Action Object** page and select the **BWM** tab.

2 In the **Bandwidth Object** field, select **Create new Bandwidth Object...**.

NOTE: Bandwidth management must be enabled or the Bandwidth Object options cannot be selected.



3 On the **General** tab, type the name of the new object in the **Name** field.

4 Set the **Guaranteed Bandwidth**. Specify either **kbps** or **Mbps**.

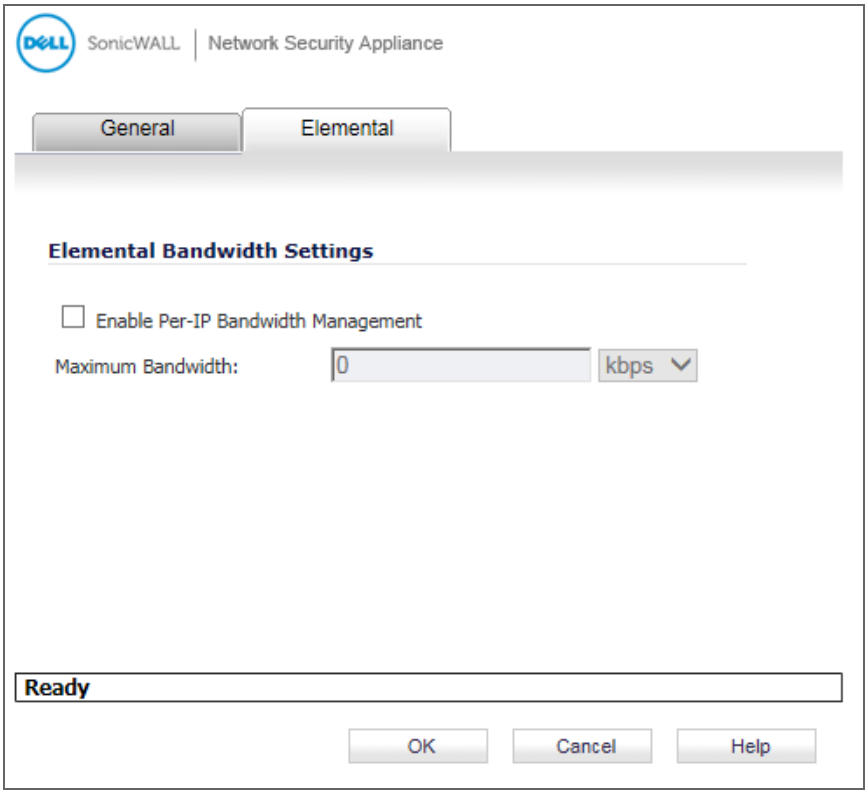
5 Set the **Maximum Bandwidth**. Specify either **kbps** or **Mbps**.

6 Set the **Traffic Priority** level from the drop-down menu. Options range from **0 Realtime** to **7 Lowest**.

7 Set the **Violation Action**. The options are **Delay** or **Drop**.

8 Add comments about these setting in the **Comments** field if you wish.

9 Select **Elemental** tab for further settings.



10 Check the box if you want to **Enable Per-IP Bandwidth Management**.

11 Specify the **Maximum Bandwidth**, in either **kbps** or **Mbps**, for elemental settings.

12 Select **OK** when all parameters have been defined.

Profile objects

A CFS profile object defines the action that is triggered for each HTTP/HTTPS connection. When setting up a new Profile Object under the new design, a domain may now be resolved to one of four ratings. From highest to lowest priority, the ratings are:

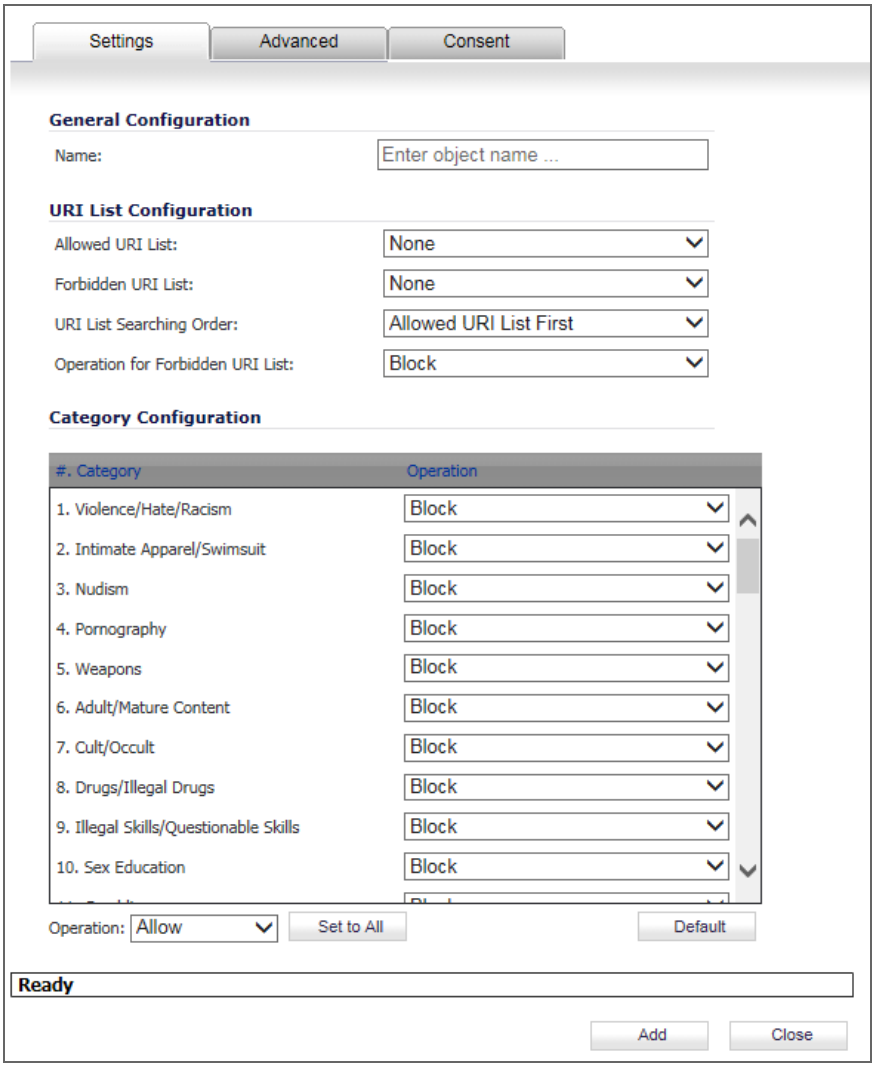
- Block
- Passphrase
- Confirm
- BWM

If the URI is not categorized into any of these ratings, then the operation is allowed.

To define a CFS Profile Object:

1 Navigate to **Firewall > Content Filter Objects**.

2 Find the **CFS Profile Objects** heading and select the **Add...** button in that section.



3 In the new window, type the name of the new object in the **Name** field.

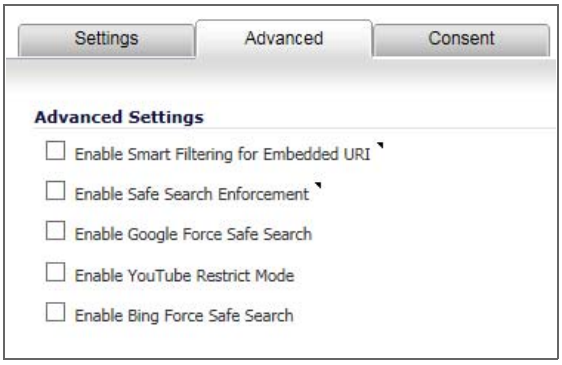
4 In the **URI List Configuration** section, set each of the following parameters:

Profile object parameters	Definition
Allowed URI list	Allows the connection if the URI is found in this list. Treat this as a white list. Choose a list object, **None**, or **Create new URI List Object**. Refer to URI List Objects for more information about creating a List Object.
Forbidden URI list	Does not allow the connection if the URI is found in this list. Treat this as a black list, and the action to be taken is defined within **Operation for Forbidden URI**. Choose a list object, **None**, or **Create new URI List Object**. Refer to URI List Objects for more information about creating a List Object.
URI List Searching Order	Specifies whether to search the **Allowed URI List First** or the **Forbidden URI List First** when validating a URI.
Operation for Forbidden URI List	Specifies what action is taken if the URI matches a URI on the Forbidden List. Choose from **Block**, **Confirm**, or **Passphrase**.

5 In the Category Configuration section, set each of the categories to **Allow**, **Block**, **BWM**, **Confirm**, or **Passphrase**. By default, Categories 1 through 12 and Category 59 are blocked; the remaining categories are allowed.

You can also easily set all categories to a single definition. In the Operation field, select **Allow**, **Block**, **BWM**, **Confirm**, or **Passphrase** and click on Set to All. Click on **Default** to restore the default settings. See Profile objects for more information.

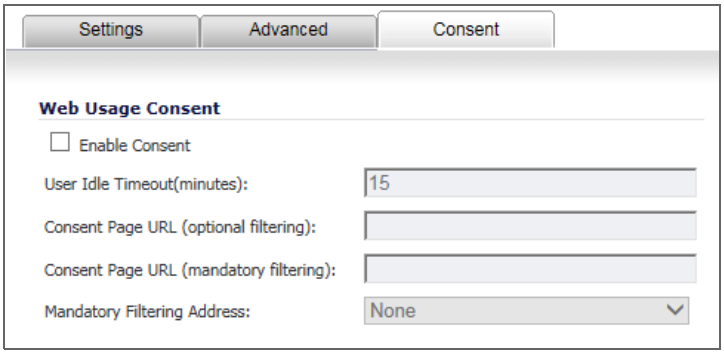
6 Go to the **Advanced** tab and check the boxes to enable the following settings. Refer to Table 1 more details on these settings.



- Enable Smart Filtering for Embedded URI
- Enable Safe Search Enforcement
- Enable Google Force Safe Search
- Enable YouTube Restrict Mode
- Enable Bing Force Safe Search

7 Go to the **Consent** tab to set up Web Usage Consent:

NOTE: Consent only works for HTTP requests. HTTPS requests cannot be redirected to the Consent page.



a Check the box to **Enable Consent**.

b Specify the **User Idle Timeout** in minutes. The default is 15 minutes.

c Fill in the field for **Consent Page URL (optional filtering)**. This is the web site where a user is redirected if they go to a website requiring consent.

d Fill in the field for **Consent Page URL (mandatory filtering)**. This is the web site where a user is redirected if they go to a website requiring mandatory filtering.

e Choose a **Mandatory Filtering Address**. Select an address group from the list or **Create New Address Object**.

8 Select **Add** when all parameters have been defined.

CFS logs

The CFS log files have been redesigned for this update. The goals was to centralize the CFS log files and streamline them. The CFS logs include:

- logstrSyslogWebSiteAccessed
- LogstrWebSiteBlocked
- logstrCFSAlert

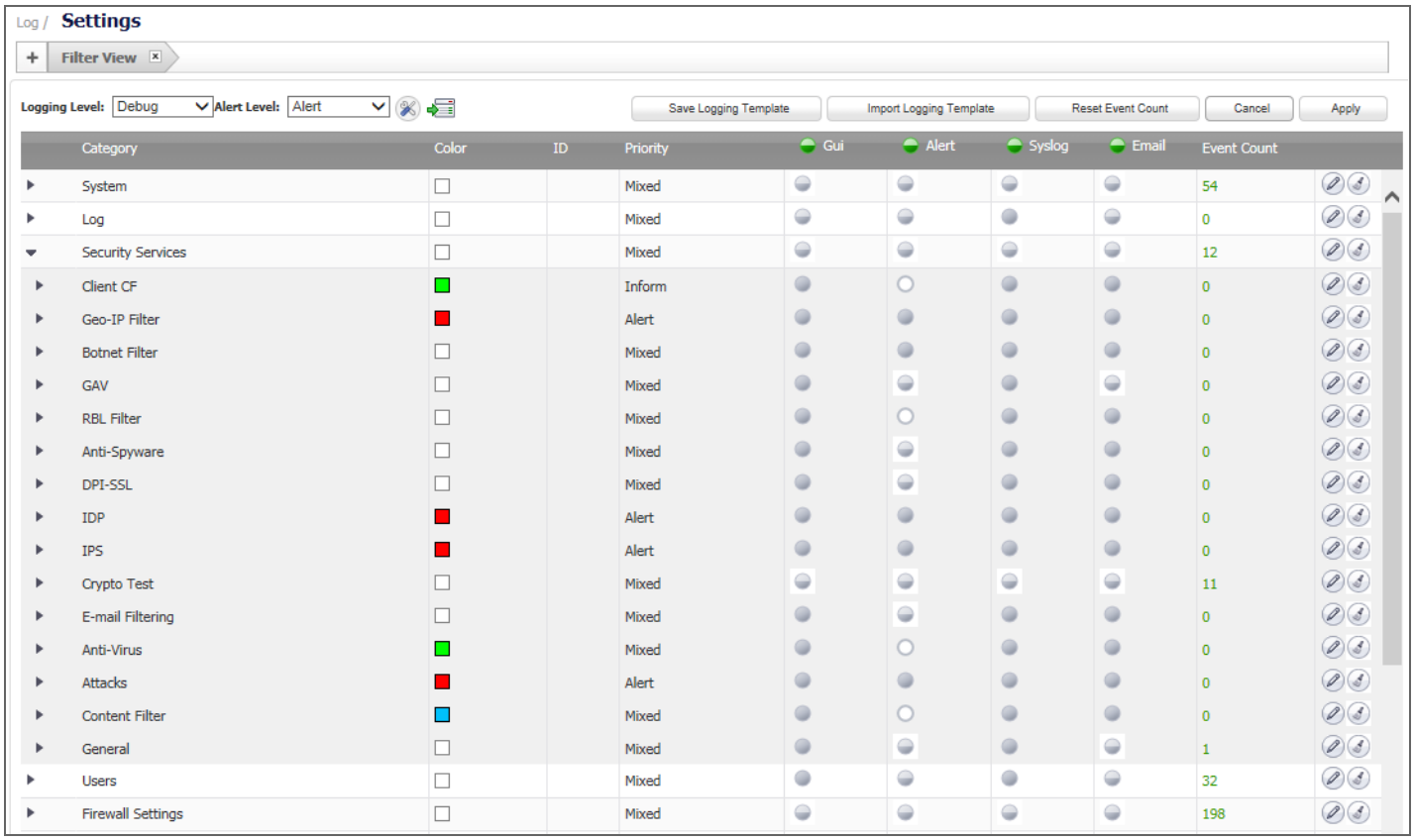
The log file logstrCFSAlert is new to this release. It records all CFS events except whether a website is accesses or blocked. Those actions are tracked in their own log files. The logs for the following functions have been deprecated:

- Appliance not registered
- Content Filter List Expired
- CFS Expiration Warning
- CFS Expiration Message
- New Group Blocked
- News Group Accessed
- ActiveX Blocked
- Java Blocked
- Archive Blocked
- Cookie Removed
- Proxy Access Blocked
- YouTube for School Enforcement

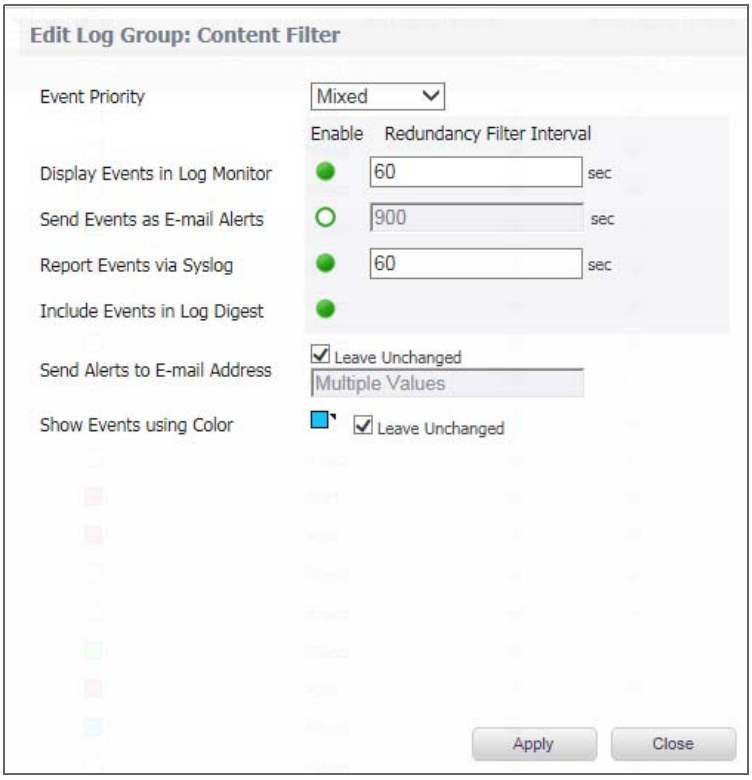
To configure the CFS logs:

1 Navigate to **Log > Settings**.

2 On the Settings page, find **Security Services** and expand it so you can see the subcategories.



3 Find **Content Filter** and select the **Edit** icon.



4 In the **Event Priority** field, select the level of event that is logged. The default is **Mixed**, but the other choices include: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Inform** and **Debug**.

5 Click the **Enable** button if you want to **Display Events in Log Monitor**, and set the **Redundancy Filter Interval**. The default interval is 60 seconds.

6 Click the **Enable** button if you want to **Send Events as E-mail Events**, and set the **Redundancy Filter Interval**. The default interval is 900 seconds.

7 Click the **Enable** button if you want to **Report Events via Syslog**, and set the **Redundancy Filter Interval**. The default interval is 60 seconds.

8 Click the **Enable** button if you want to **Display Events in Log Monitor**.

9 Choose whether you want to **Send Alerts to Email Address**. The default is to check the box to **Leave Unchanged**. If you uncheck the box, you can add the email address of the person or group you want to receive the alerts.

10 Choose whether you want to **Show Events using Color**. The default is for no color, but if you uncheck the **Leave Unchanged** box, you can select a color and CFS events appear in the log file in that color.

11 When all options are defined, select **Apply**.

Comparison of CFS

The following table compares the user experience for various aspects of the old and new CFS.

CFS 3.0	CFS 4.0
Configure CFS on CFS page, Zone page, User page, and App Rules page.	Centralized CFS configuration in one place.
Two modes (via Zones and via App Rules)	Merged functions into one mode

CFS 3.0	CFS 4.0
Admin cannot predict the filtering results accurately after configuration.	Admin can exactly predict the filtering results.
Need to define duplicated filtering options.	Define CFS Category definitions, URI List Object, Profile Object and Action Object, which can be reused in multiple policies.
Does not support wildcard matching.	Supports wildcard (*) matching for URI List Objects.
Consent feature is global.	Consent feature is per policy.
BWM is only supported in App Rules mode.	BWM is fully supported.
Does not support Override - Confirm.	Supports override through Passphrase and supports confirm.
Only supports GET, POST, and HEAD commands for HTTP.	supports GET, POST, HEAD, PUT, CONNECT, OPTIONS, DELETE, REPORT, COPY and MOVE commands.
Cannot enable/disable CFS globally.	Can enable/disable CFS globally.
Custom category is based on category.	Custom category is based on domain, which is more intuitive.
Websense configuration is mixed with CFS configuration.	Separate Websense configuration from CFS configuration helps prevent errors.

Supported platforms

These are supported Dell SonicWALL appliances for CFS 4.0:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless
- TZ400 and TZ400 Wireless
- TZ300 and TZ300 Wireless
- SOHO Wireless

Product licensing

CFS 4.0 can be licensed in two ways: through MySonicWALL or from a firewall user interface. If you want to upgrade an existing license, refer to *SonicOS 6.2.6 Content Filtering Service (CFS) 4.0 Upgrade Guide* for details.

Licensing in MySonicWALL

To license in MySonicWALL:

1. Log into MySonicWALL from a web browser.
2. Click **My Products** in the left navigation menu.
3. Locate the registered appliance that you want to license for CFS and click on its friendly name or serial number.
4. On the **Service Management** page, scroll down to the **Applicable Services** section and locate **Content Filtering: Premium Edition**.

5 Do one of the following:

- Click the **Buy** button to purchase a service license.
- Click the **Activate** button if you already have a license key from your SonicWALL distributor or from a previous transaction.

6 Follow the prompts to complete the license activation. On your appliance, the CFS license status is indicated on the **System>Status** and **System>Licenses** pages in SonicOS.

7 If CFS appears as unlicensed, click the Synchronize button on the **System>Licenses** page to update the status.

Licensing from a firewall

To license from a firewall:

1 On a registered Dell SonicWALL firewall, navigate to the **System > Licenses** page.

2 Scroll down to the **Manage Security Services Online** section, click the link in **To Activate, Upgrade, or Renew services, click here**.

3 Enter your MySonicWALL credentials to log in and open the **Service Management** page.

4 Scroll down to the **Applicable Services** section and locate the **Content Filtering: Premium Edition**.

5 Click either the **Buy or Activate** button to license the **Content Filtering: Premium Edition**. On your firewall, the **System** > **Status** page displays the updated license status.

6 Follow the prompts to complete the license activation. Upon completion you are returned to the **System>Licenses** page in SonicOS. The **System>Status** page also displays the updated license status.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit http://www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.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:

- Create, update, and manage Service Requests (cases).
- View Knowledge Base articles.

- Obtain product notifications.
- Download software. For trial software, go to http://software.dell.com/trials.
- View how-to videos.
- Engage in community discussions.
- Chat with a support engineer.

Copyright© 2016 Dell Inc.
ALL RIGHTS RESERVED.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and SonicWALL™ are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

For more information, go to http://software.dell.com/legal/.

Legend

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

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

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

CFS Feature Guide
Updated - August 2016
Version - 4.0
232-003341-00 Rev A