SonicOS 7.1

Content Filtering

Administration Guide

Contents

1

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses onSonicWall's Content Filtering Service's (CFS) ability to compare requested web sites against a massive database in the cloud that contains millions of rated URLs, IP addresses, and web sites. This service provides you 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, for over 50 predefined categories.

Topics:

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

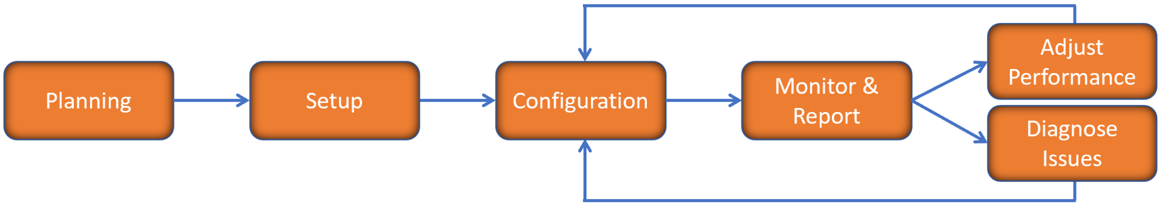
Firewall Type	**Classic Mode**	**Policy Mode**	**Comments**
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTPPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls. For more information, refer to:

- SonicOS 7.1 API Reference Guide
- *SonicOS Command Line Interface Reference Guide*

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

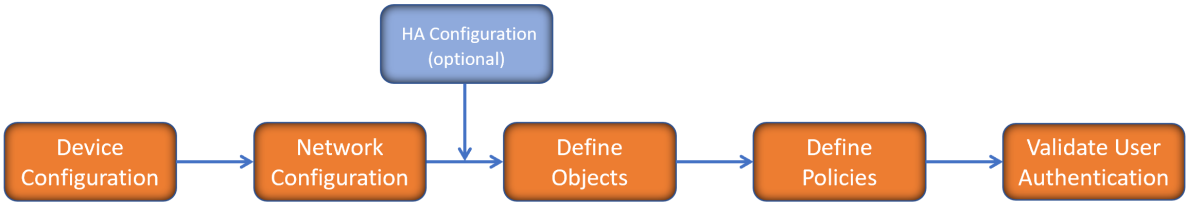


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

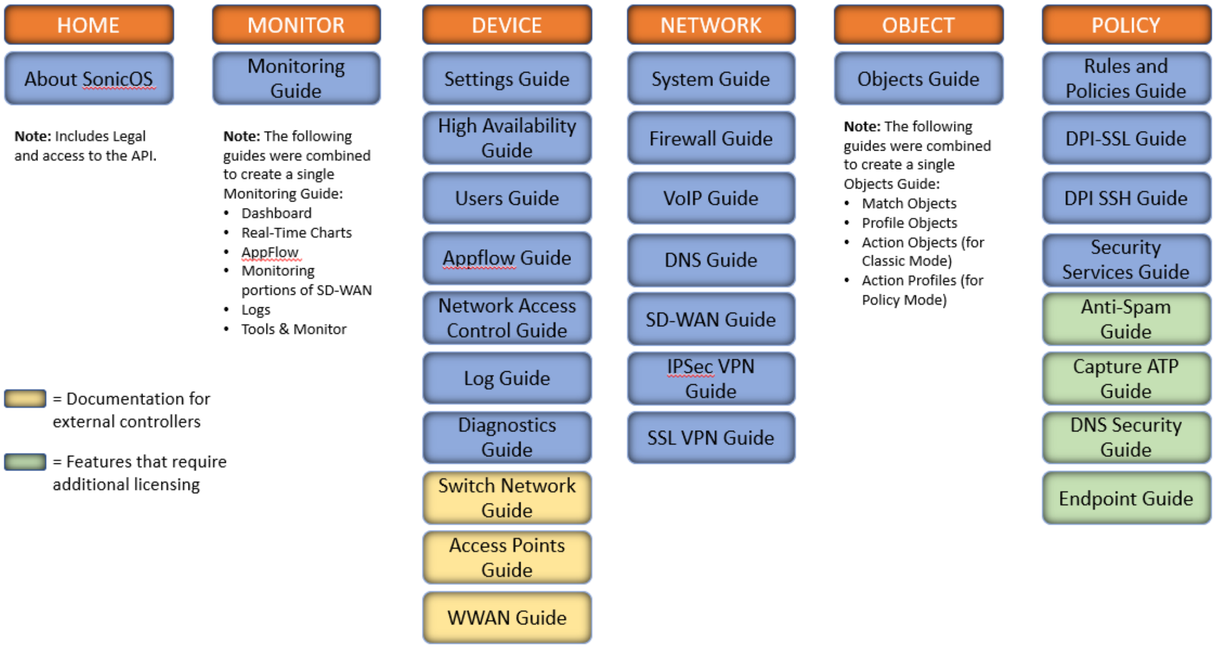


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 7.1 Monitor Guide and the SonicOS 7.1 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



Note: Includes Legal and access to the API.

Note: The following guides were combined to create a single Monitoring Guide:

- Dashboard
- Real-Time Charts
- AppFlow
- Monitoring portions of SD-WAN
- Logs
- Tools & Monitor

Note: The following guides were combined to create a single Objects Guide:

- Match Objects
- Profile Objects
- Action Objects (for Classic Mode)
- Action Profiles (for Policy Mode)

🟨 = Documentation for external controllers

🟩 = Features that require additional licensing

The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the https://www.sonicwall.com/support/technical-documentation/.

Guide Conventions

These text conventions are used in this guide:

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **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.**

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function | Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, **NETWORK | System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page.
`Code`	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=**<*your serial number*>, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

2

Content Filtering Service 5.0

SonicWall offers comprehensive web content security that blocks selected web content and enforces protection and productivity policies. Content Filtering Service (CFS) protects the devices behind the firewall and provides administrators with the means to define and manage policies for groups or individual users.

Topics:

- CFS Overview

CFS Overview

URL filtering is becoming a commodity with basic requirements for blocking, based on business objectives and threat reputation. The SonicWall Content Filtering Service targets these issues and has been updated to provide more web categories to screen and a new filter so URLs can be filtered by reputation. The Reputation feature calculates a score that forecasts the security risk of a URL so you can determine how best to categorize and respond to it.

You configure Content Filtering Service settings in SonicOS. The SonicWall Content Filtering Service is available with both the Essential Protection Service Suite and the Advanced Protections Service Suite. With a valid subscription, you can create custom CFS policies and apply them to network zones or to groups of users within your organization. You can enforce policy rules for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites users can access using their IT-issued computers while behind the organization's firewall.

The general process for setting up and enabling Content Filtering Service is:

1. Enable Content Filtering Service.

   Some basic Content Filtering capability is provided, but it can be customized and expanded beyond the default tools provided. Navigate to **POLICY | Security Services > Content Filter** to enable the service. For more information, refer to Configuring Content Filtering Service.

2. Define the profile objects for Content Filtering.

   A **Profile Object** defines what kind of operation can be triggered for each HTTP/HTTPS connection. Navigate to **OBJECT | Profile Objects > Content Filter** to edit the CFS Default Profile or add customized Content Filtering profile objects. For more information, refer to Defining Profile Objects.

3. Define the action objects for Content Filtering.

   An **Action Object** defines what happens after a packet is filtered by CFS. Navigate to **OBJECT | Action Objects > Content Filter Actions** to edit or define action objects. For more information, refer to Configuring CFS Action Objects.

4. Define the reputation object for Content Filtering.

   A **Reputation** is an **Action Object** that defines the action to take based on the reputation of a URL. A CFS Default Reputation Object is provided, but you can create customized Reputation Objects. For more information, refer to Configuring CFS Action Objects .

5. Define the policies for how to filter and respond to web content that users access.

   A default policy provides standard settings for content filters, but with additional licensing, you can create customized policies to manage different user scenarios. Navigate to **POLICY | Rules and Policies > Content Filter Rules** to define policies. For more information, refer to Configuring CFS Policies and Rules.

3

Configuring Content Filtering Service

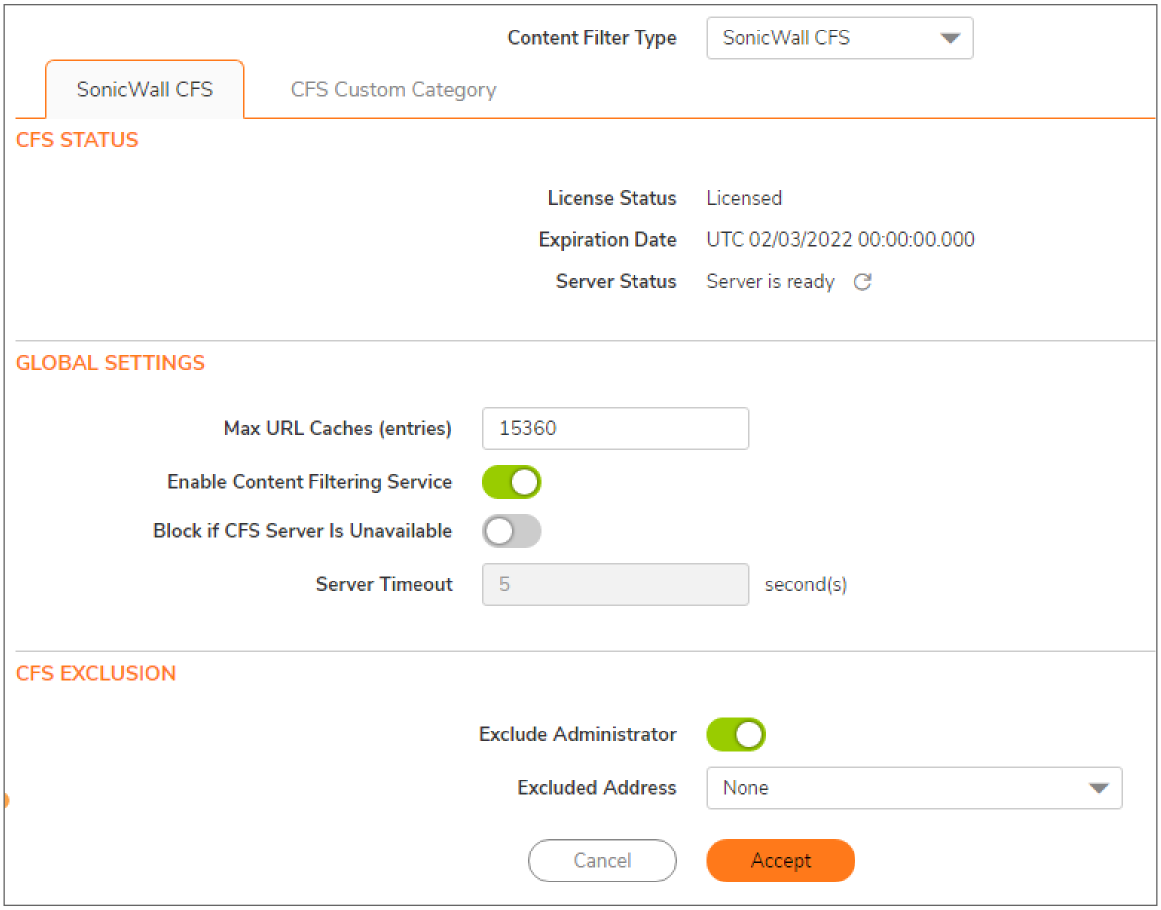
The Content Filtering Service is a part of the Security Services options that SonicWall offers to help you secure your environment. The Content Filtering Service provides a default Profile Object and reputation-based Action Object for minimal coverage. You can create customized objects and policies to increase the coverage.

- Configuring the SonicWall CFS Tab
- Configuring the CFS Custom Category Tab

Configuring the SonicWall CFS Tab

To enable and configure Content Filtering:

1. Navigate to **POLICY | Security Services > Content Filter**.



Content Filter Type: SonicWall CFS

CFS STATUS

License Status: Licensed
Expiration Date: UTC 02/03/2022 00:00:00.000
Server Status: Server is ready

GLOBAL SETTINGS

Max URL Caches (entries): 15360
Enable Content Filtering Service: ●
Block if CFS Server Is Unavailable: ○
Server Timeout: 5 second(s)

CFS EXCLUSION

Exclude Administrator: ●
Excluded Address: None

2. Define the settings on the two tabs of this window and click **Accept**.

   The default tab, **SonicWallCFS** is separated into three sections, providing status and options to set.

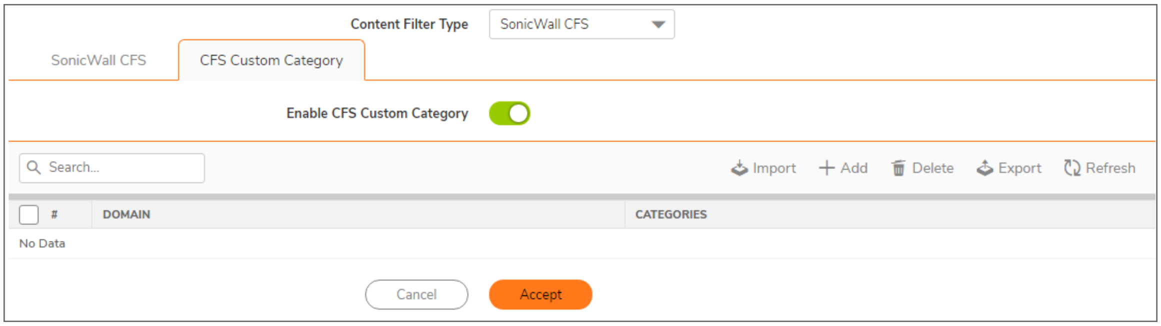
CFS Status	Shows: • **License Status**—states whether Content Filtering is licensed or not. • **Expiration Date**—displays the expiration date for your CFS subscription. • **Server Status**—displays the server status. Click **Refresh** to refresh the server status.

Global Settings	Lists several settings you can define for CFS behavior: • Enter the maximum number of URL cache entries allowed. The minimum is 25,600 and the maximum is 51,200, although the range might vary depending on the size of your firewall. • Click the switch to green to **Enable Content Filtering Service**. • Click the switch to green to **Block if CFS Server is Unavailable**. • Set the **Server Timeout**, in seconds, if **Block if CFS Server is Unavailable** is enabled. The minimum is two seconds, the maximum is 10 seconds, and the default is five seconds. The **Server Timeout** option is not editable if it is not enabled.
CFS Exclusion	Lists options that allow packets from the administrator and a number of address objects to pass through unfiltered. • Click the switch to green if you want to **Exclude Administrator** packets. • Click the drop-down menu if you want to **Exclude Address**. Select a specific type of address or address object from the drop-down menu. You can also create an address object or address group by selecting the appropriate option from the drop-down menu.

3. Click **Accept** to save the configuration options you set.

Configuring the CFS Custom Category Tab

The CFS Custom Category tab allows the configuration of new custom CFS category entries. You can create custom policies and categories and insert the domain name entries into the existing CFS rating category structure. Categories are added and deleted from this page.



Content Filter Type SonicWall CFS

Enable CFS Custom Category

☐	#	DOMAIN	CATEGORIES

No Data

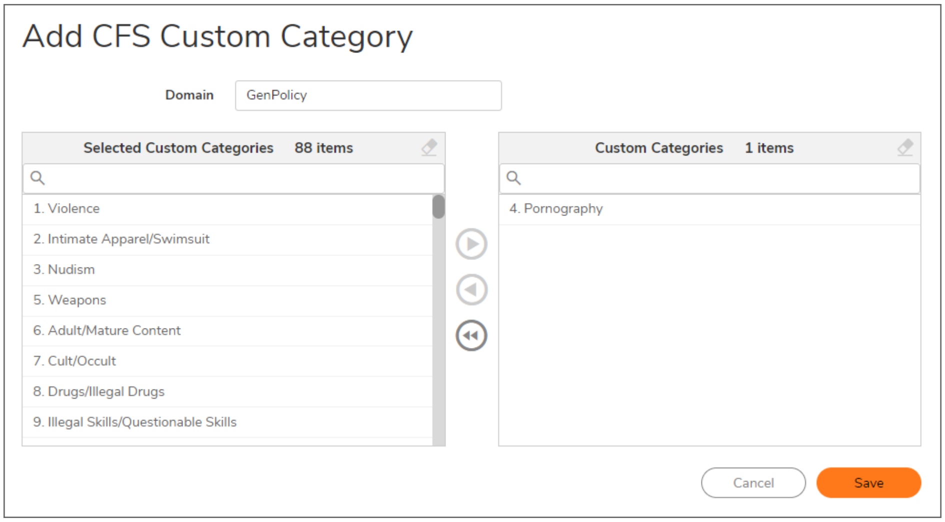
- Click the switch to green to **Enable CFS Custom Category**.
- Click **+Add** to create a new custom category.
- Select the category and click **Delete** to remove a category.
- Click **Export** to export the current list of categories. You can edit this list offline if you need to make

multiple updates and import it back to the firewall.

- Click **Import** to import a predefined set of categories.

To create a new category:

1. Navigate to **POLICY | Security Services > Content Filter** and select the **CFS Custom Category** tab.
2. Click **+Add**.



Add CFS Custom Category

Domain: GenPolicy

Selected Custom Categories 88 items

1. Violence
2. Intimate Apparel/Swimsuit
3. Nudism
5. Weapons
6. Adult/Mature Content
7. Cult/Occult
8. Drugs/Illegal Drugs
9. Illegal Skills/Questionable Skills

Custom Categories 1 items

4. Pornography

3. Type a name in the **Domain** field.
4. Select a category from the list on the left and move it to the custom categories on the right. Up to five custom categories can be selected.
5. Click **Save**.

To delete a custom category:

1. Navigate to **POLICY | Security Services > Content Filter** and select the **CFS Custom Category** tab.
2. Select the custom category by checking the box by **DOMAIN**.
3. Click the **Delete** icon.
4. Confirm your choice to delete by clicking **OK**.

To export the CFS Category list:

1. Click **Export** to export the category list to a text file. The exported file is placed in the downloads folder.

The exported file can be used to update multiple entries. Edit the file and import the new file following the following procedure.

ⓘ **NOTE:** When editing an exported list, be sure to follow the format of the list: <*domain*>: <*category1*>, <*category2*>, <*category3*>, *category4*>, <*category5*>

To import multiple categories simultaneously:

IMPORTANT: All the custom categories already in the list are deleted when a list of categories are uploaded.

1. Click **Import**.

   ⓘ | **NOTE:** Invalid domain names and category IDs in the importing file are skipped.

   ⓘ | **NOTE:** The leading www. of any domain name is discarded during processing.

2. Type the file name in field provided, or **Browse** for the file and select it on your system.
3. Click **Import**.

4

Defining Profile Objects

A Profile Object defines what kind of operation is triggered for each HTTP/HTTPS connection. You can define what is allowed, what is blocked, and what is forbidden. You can also define the operations for each category (Allowed, Blocked, Confirm, Passphrase, and BWM).

The CFS Default Profile is provided with your license. You can edit it to customize the settings but you can't delete it. You can also add other CFS profiles and customize them to meet specific filtering requirements. To define a Profile Object, navigate to **OBJECT | Profile Objects > Content Filter** of the firewall interface.

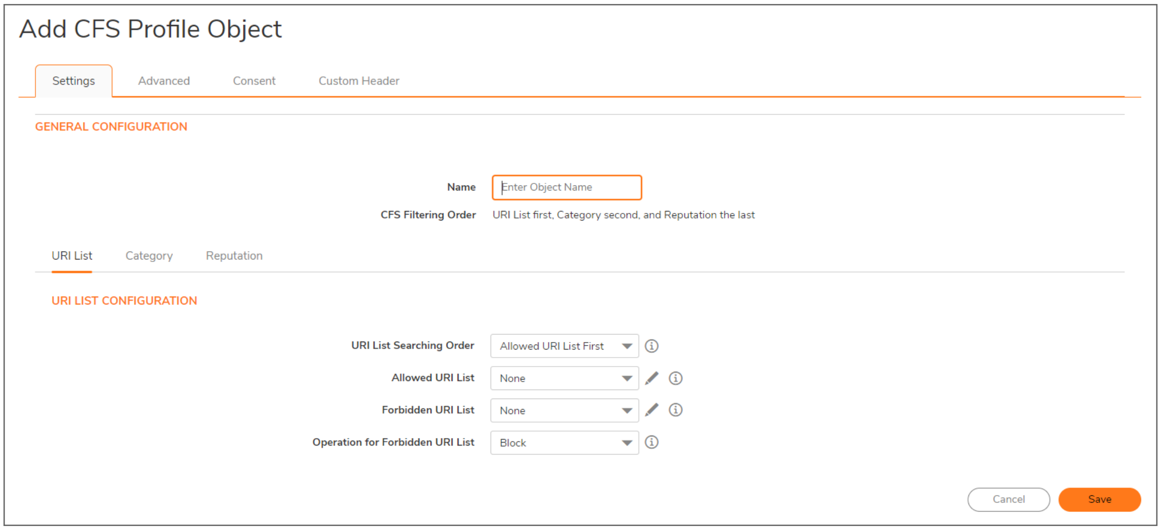
Topics:

- Creating or Editing a Profile Object
  - Advanced Settings
  - Consent
  - Custom Header
  - Creating a New URI List Object
- Editing Profile Objects
- Deleting Profile Objects

Creating or Editing a Profile Object

To add a Project Object for Content Filtering:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Click **+Add**.



Add CFS Profile Object

GENERAL CONFIGURATION

Name: Enter Object Name

CFS Filtering Order: URI List first, Category second, and Reputation the last

URI LIST CONFIGURATION

URI List Searching Order: Allowed URI List First

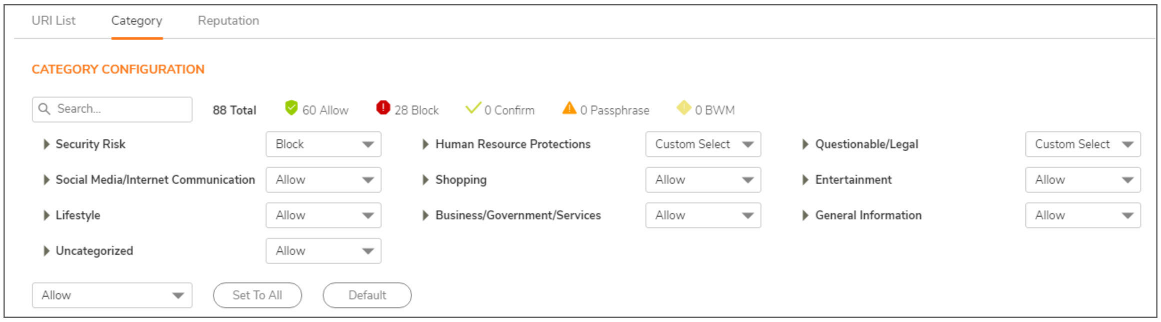
Allowed URI List: None

Forbidden URI List: None

Operation for Forbidden URI List: Block

3. Enter the Profile Object Name in the **Name** field.
4. In the **URI List Configuration** section, define the parameters for **URI List**:
   a. Select the **URI List Searching Order** from the drop-down menu provided. You can select the allowed list first or the forbidden list first.
   b. Select the **Allowed URI List** from the drop-down menu. Accessing all the URIs in this list is allowed.
   c. Click the **Edit** icon next to the**Allowed URI List** field to create a **New URI List Object**. For more information, refer to Creating a New URI List Object.
   d. Select the **Forbidden URI List** from the drop-down menu. Accessing all the URIs in this object is forbidden.
   e. Click the **Edit** icon next to the**Forbidden URI List** field to create a **New URI List Object**. For more information, refer to Creating a New URI List Object .
   f. Select the **Operation for Forbidden URI List** in the drop-down menu. The selected action—**Block**, **Confirm**, or **Passphrase**—applies for all URIs in the forbidden list.

5. Click the **Category** tab to define the **Category Configuration** section. You can customize the categories to fit your environment. The option are **Allow**, **Block**, **Confirm**, **Passphrase**, and **BMW**.



CATEGORY CONFIGURATION

88 Total ✓ 60 Allow ● 28 Block ✓ 0 Confirm ⚠ 0 Passphrase ◆ 0 BWM

Security Risk	Block	Human Resource Protections	Custom Select	Questionable/Legal	Custom Select
Social Media/Internet Communication	Allow	Shopping	Allow	Entertainment	Allow
Lifestyle	Allow	Business/Government/Services	Allow	General Information	Allow
Uncategorized	Allow				

Allow

a. Expand the category name to see the details under it.

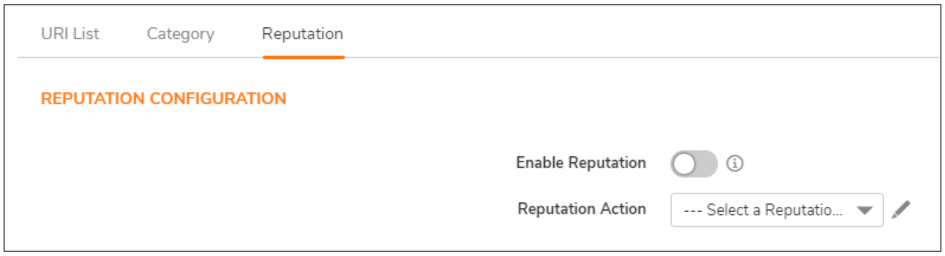
b. If you want the same definition for everything in the category, select the action from the drop-down menu for the category name.

c. If you want to customize the category, select the action from the drop-down menu for each item. Note how the category action is changed to **Custom Select**.

d. If you want all categories defined the same, select the action from the drop-down menu at the bottom of the page and click **Set To All**.

e. Click **Default** to reset all options to the default settings.

6. Select **Reputation**to define the **Reputation Configuration** section. Filtering by reputation must be enabled and is used only on categories that are **Allowed**.



REPUTATION CONFIGURATION

Enable Reputation ○

Reputation Action: --- Select a Reputatio...

a. Switch **Enable Reputation** to green.

b. Select **Reputation Action** from the drop-down menu for each option.

> **NOTE:** You can select the **Edit** icon by the drop-down menu to create a new **Reputation Action Object** to choose from the list.

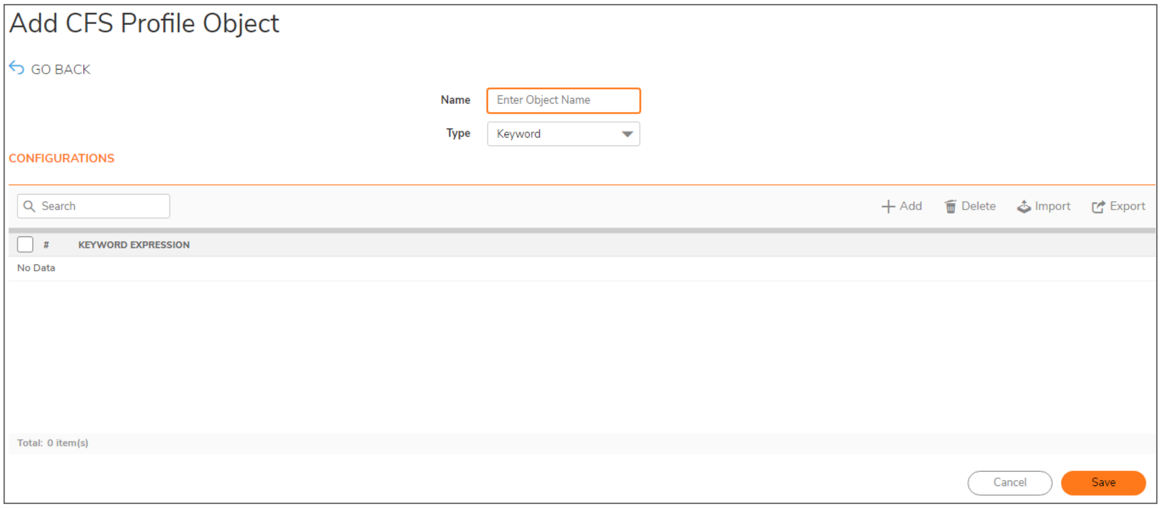
7. When all settings have been defined, click **Save**.

Creating a New URI List Object

URI List Objects can be created for both the Allowed URI List and the Forbidden URI List.

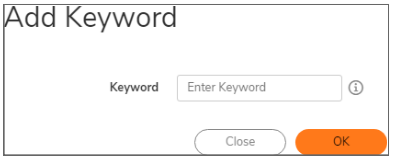
To create a URI List Object:

1. Click the **Edit** icon next to the **Allowed** or **Forbidden URI List** field.



Type: Keyword

2. **Name** the List Object.
3. Select the **Type** of object from the drop-down menu. The options are **Domain**, **Keyword**, or **URI**.
4. Click **+Add** to create a Domain, Keyword or URI. The following shows the Keyword option.



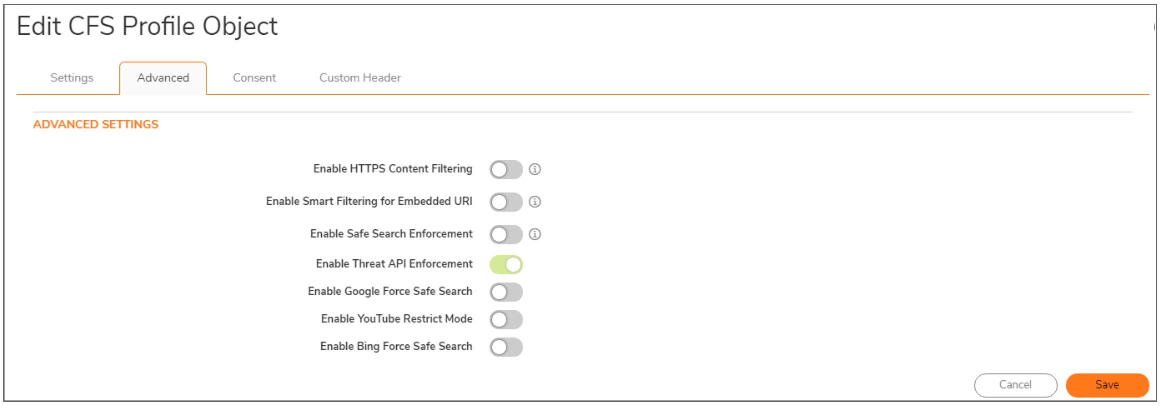
5. Enter the appropriate text in the field. Multiple entries can be separated with a semicolon.
6. Click **OK**.
7. Click **Save**.

Advanced Settings

You can define a series of advanced settings to further define your CFS Profile Object. These appear on a separate tab when you add or edit a CFS Profile Object. You can define the advanced settings when creating the object or you can set them later.

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Click **+Add**.

3. Click the **Advanced** tab.



Edit CFS Profile Object

ADVANCED SETTINGS

Enable HTTPS Content Filtering ○
Enable Smart Filtering for Embedded URI ○
Enable Safe Search Enforcement ○
Enable Threat API Enforcement ●
Enable Google Force Safe Search ○
Enable YouTube Restrict Mode ○
Enable Bing Force Safe Search ○

4. Click the switch to green to **Enable HTTPS Content Filtering**. HTTPS content filtering is IP based, and does not inspect the URL. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages are silently blocked.
5. Click the switch to green to **Enable Smart Filtering for Embedded URI**. This feature currently only applies to Google Translate, and it requires that DPI-SSL be enabled along with Content Filtering. This option is disabled by default.

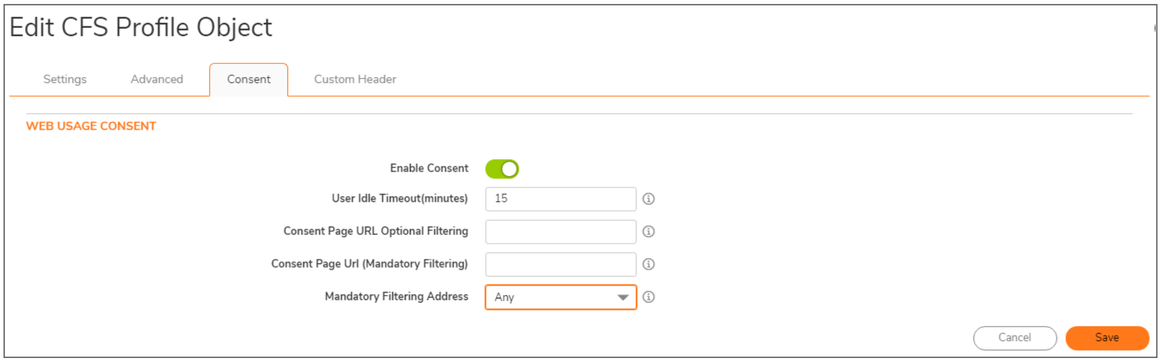
   ⓘ | **NOTE:** The DPI-SSH Client SSL is set on the **General** tab at **POLICY | DPI-SSL > Client SSL**.
6. Click the switch to green to **Enable Safe Search Enforcement**.This feature currently only applies to Yahoo and Dogpile, and for HTTPS sites, it requires that DPI-SSL be enabled along with Content Filtering, as noted above. This option is disabled by default.
7. Click the switch to green to **Enable Google Force Safe Search**.
8. Click the switch to green to **Enable YouTube Restrict Mode**.
9. Click the switch to green to **Enable Bing Force Safe Search**.
10. Click **Save** when done.

Consent

You can require consent to access certain web pages as a part of your CFS Profile Object. These appear on a separate tab when you add or edit a CFS Profile Object. You can enable **Consent** when creating the object or you can set those parameters later.

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Click **+Add**.

3. Click the **Consent** tab.



Edit CFS Profile Object

WEB USAGE CONSENT

Enable Consent: on

User Idle Timeout(minutes): 15

Consent Page URL Optional Filtering:

Consent Page Url (Mandatory Filtering):

Mandatory Filtering Address: Any

4. Click the switch to green to **Enable Consent**.
5. Set the **User Idle Timeout** in minutes. This feature reminds users that their time has expired by displaying the page defined in the Consent page URL. Minimum idle time can be as low as one minute, but as high as 9999 minutes. The default is set to 15 minutes.
6. In the **Consent Page URL Optional Filter** field, list the URL that the user is redirected to when he or she opens a web site that requirements consent. This page must reside on a Web server and be accessible as a URI by users on the network.

   > ⓘ **IMPORTANT:** The consent page must contain links to two SonicWall pages, which, when selected, tell the appliance that the user wishes to have filtered or unfiltered access. The link for unfiltered access is: `192.168.168.168/iAccept.html`. The link for filtered access is `192.168.168.168/iAcceptFilter.html`. Use the LAN IP of the appliance for the link root.

7. In the **Consent Page URL (Mandatory Filtering)** field, list the URL that the user is redirected to when he or she opens a web site with mandatory filtering. This page must reside on a Web server and be accessible as a URI by users on the network.

   > ⓘ **IMPORTANT:** The mandatory filtering page must contain the following SonicWall link, which, when selected, tells the appliance that the user accepts filtered access. The link for filtered access is: `192.168.168.168/iAcceptFilter.html`. Use the LAN IP of the appliance for the link root.

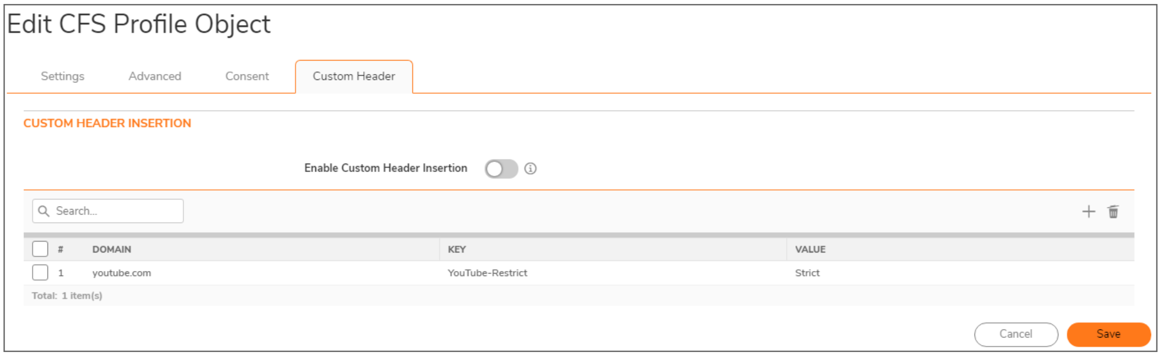
8. Select the **Mandatory Filtering Address** from the drop-down menu. All configured IP addresses associated with a selection or object require mandatory filtering.
9. Click **Save**.

Custom Header

Content Filtering can be enabled so that a header configured by customers can be added to HTTP and HTTPS requests. For HTTPS requests, DPI-SSL functionality must also be enabled. By default the **Custom Header** is disabled.

To set up a Custom Header:

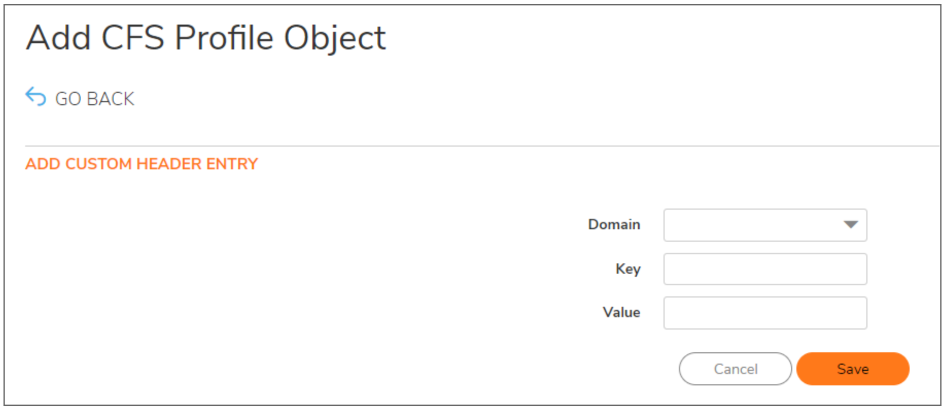
1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Click **+Add**.
3. Click the **Custom Header** tab.



#	DOMAIN	KEY	VALUE
1	youtube.com	YouTube-Restrict	Strict

Total: 1 item(s)

4. Click the switch to green to **Enable Custom Header Insertion**.
5. Click the **Add** icon (**+**) to add a new **Custom Header Entry**.



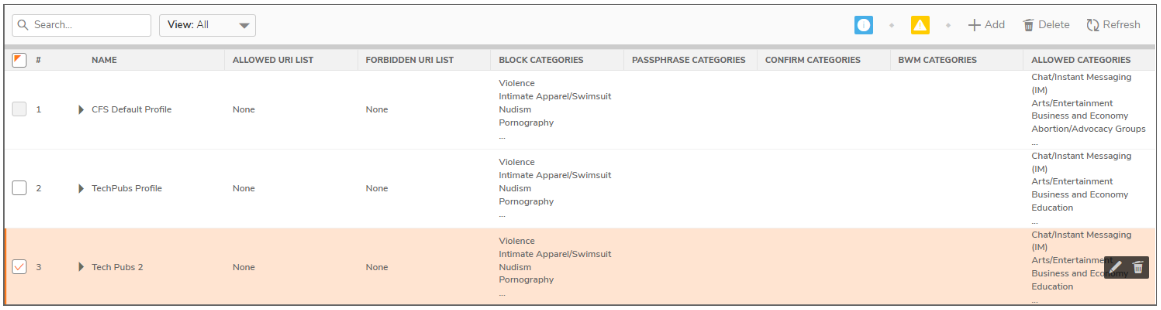
6. Select **Domain** from the drop-down menu. The **Key** and **Value** fields are automatically filled in based on your selection.
7. Click **Save** to save the **Custom Header Entry**.
8. Click **Save** to save the **Custom Header** settings.

Editing Profile Objects

Editing an object profile is very similar to creating one.

To edit a CFS profile object:

1. Navigate to **Object | Proficle Objects > Content Filter**.
2. Select the object you want to edit.



Search... | View: All | + Add | Delete | Refresh

☑	#	NAME	ALLOWED URI LIST	FORBIDDEN URI LIST	BLOCK CATEGORIES	PASSPHRASE CATEGORIES	CONFIRM CATEGORIES	BWM CATEGORIES	ALLOWED CATEGORIES
□	1	CFS Default Profile	None	None	Violence Intimate Apparel/Swimsuit Nudism Pornography ...				Chat/Instant Messaging (IM) Arts/Entertainment Business and Economy Abortion/Advocacy Groups ...
□	2	TechPubs Profile	None	None	Violence Intimate Apparel/Swimsuit Nudism Pornography ...				Chat/Instant Messaging (IM) Arts/Entertainment Business and Economy Education ...
☑	3	Tech Pubs 2	None	None	Violence Intimate Apparel/Swimsuit Nudism Pornography ...				Chat/Instant Messaging (IM) Arts/Entertainment Business and Economy Education ...

3. Click the **Edit** icon, which appears to the far right of the screen.
4. Navigate the options (**URI List**, **Category**, **Reputation**) on the **Settings** window to make the changes needed.
5. Navigate through the other tabs—**Advanced**, **Consent**, **Custom Header**—to made the the changes needed there.
6. Click **Save** when done.

Deleting Profile Objects

Several different options are provided for deleting a Content Filtering Profile Object. However you do it, you are asked to confirm that you really want to delete the item.

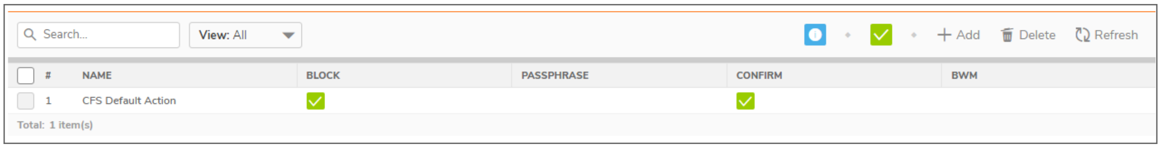
- You can select an individual profile object by checking the box and clicking the **Delete** icon at the top or in the row you selected.
- You can simply highlight a row in the table and click the **Delete** icon at the end of the row you selected.
- You can select multiple profile objects by checking the boxes and clicking the **Delete** icon at the top.

ⓘ | **NOTE:** The **CFS Default Profile** cannot be deleted.

5

Configuring CFS Action Objects

The CFS Action Object defines what happens after a packet is filtered by CFS and matches a CFS policy. SonicWall provides the CFS Default Action object. This object cannot be deleted but you can edit it and customize some of the settings. You can also add and delete customized action objects for CFS. To configure CFS Action Objects, navigate to **OBJECT | Action Objects > Content Filter Actions**.



□	#	NAME	BLOCK	PASSPHRASE	CONFIRM	BWM
□	1	CFS Default Action	✓		✓	

Total: 1 item(s)

Topics:

- Adding or Editing CFS Action Objects
- Deleting Action Objects

Adding or Editing CFS Action Objects

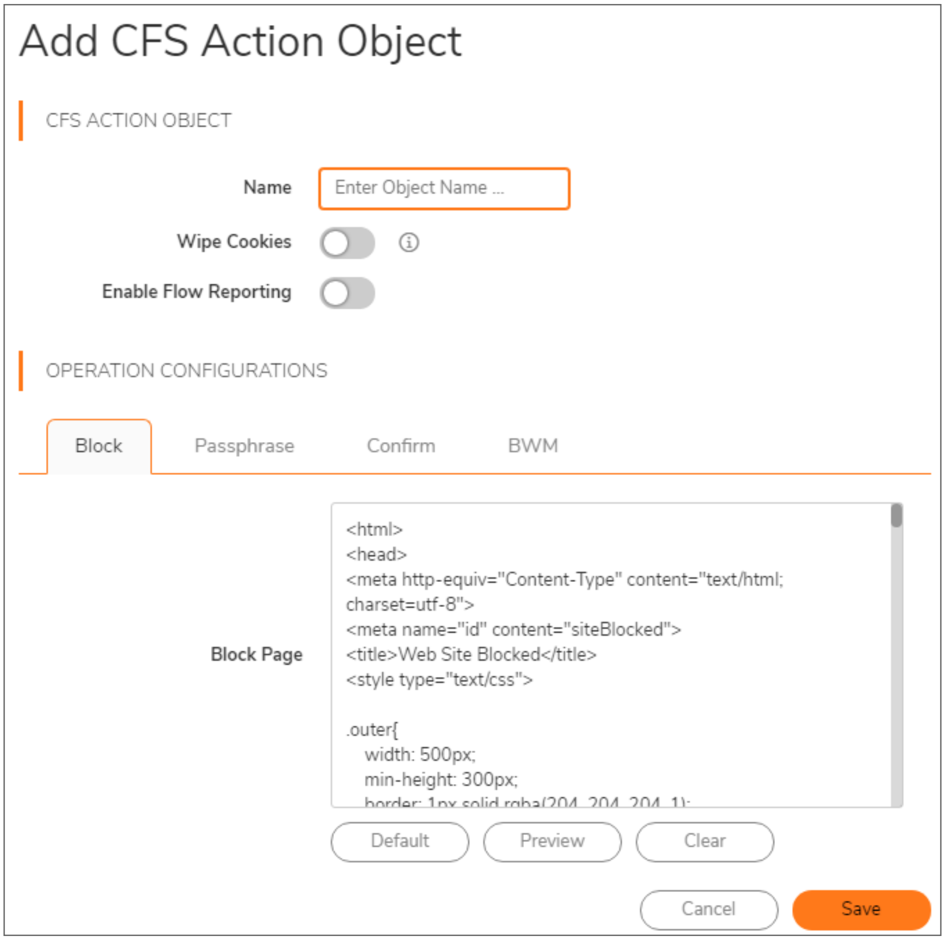
Adding and editing an action object is very similar. The following procedures describe the options you can set in either instance.

To add a Project Object for Content Filtering:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Click **+Add**.

To edit a Project Object for Content Filtering:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Highlight the action object and click the **Edit** icon.



```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
<meta name="id" content="siteBlocked">
<title>Web Site Blocked</title>
<style type="text/css">

.outer{
   width: 500px;
   min-height: 300px;
   border: 1px solid rgba(204, 204, 204, 1);
```

To set or change the parameters for a CFS Action Object:

1. Open the **CFS Action Object** window as previously described.
2. Enter or edit the action object **Name** in the field provided.

   ⓘ | **NOTE:** The name of the **CFS Default Action** cannot be changed.

3. Click the switch to green to **Wipe Cookies**.This feature takes affect for HTTPS sites, only when Content Filter is enabled for the DPI-SSLClient SSL.

   ⓘ | **NOTE:** The DPI-SSL Client SSL is set on the **General** tab at (missing or bad snippet).

   ⓘ | **IMPORTANT:** If the Wipe Cookies options is enabled, it could break the Safe Search Enforcement function for some search engines.

4. Click the switch to green to **Enable Flow Reporting**.This feature allows CFS flow data to be collected for analysis.

5. In the **Block** tab of the **Operations Configurations** section, define the HTML for the blocked page you want to display.

    a. Input or edit the HTML in the field provided.

    b. Click **Default** to reset the page to the default HTML code.

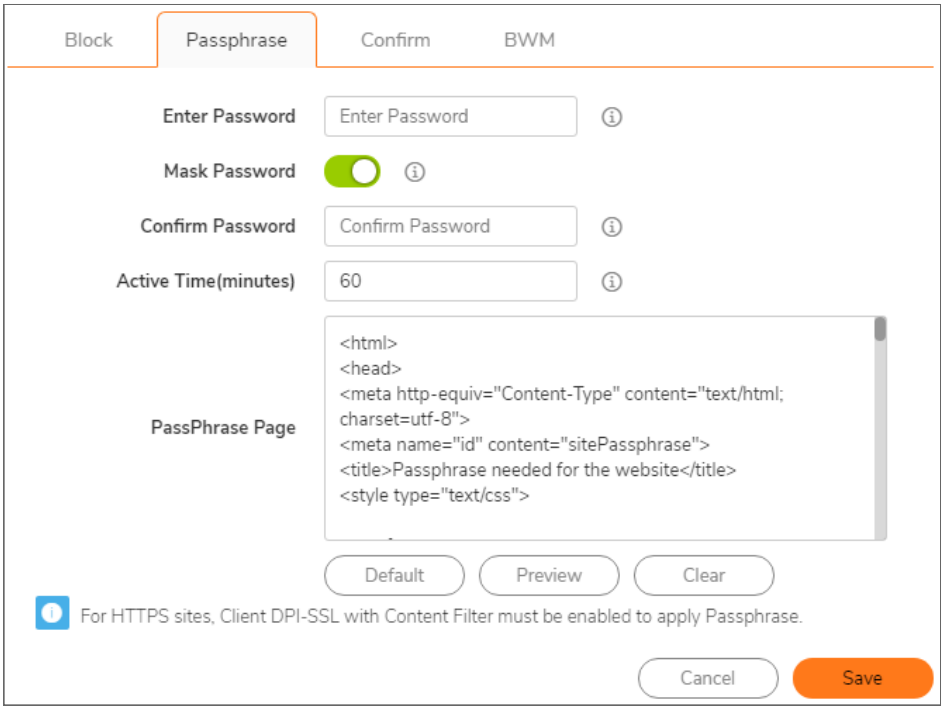
    c. Click **Preview** see what is displayed when a URI is blocked.

    d. Click **Clear** to clear the **Block Page** text block and start over.

    e. Click **Save** to save the settings.

6. In the **Passphrase** tab of the **Operations Configurations** section, define the settings for requiring a passphrase when certain URIs are detected.

    ⓘ | **NOTE:** For HTTPS sites, the Content Filtering option for the DPI-SSL Client SSL must be enabled to for **Passphrase** to work. Navigate to the **General** tab at **POLICY | DPI-SSL > Client SSL** to set this.



Enter Password: Enter Password

Mask Password: on

Confirm Password: Confirm Password

Active Time(minutes): 60

PassPhrase Page:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
<meta name="id" content="sitePassphrase">
<title>Passphrase needed for the website</title>
<style type="text/css">
```

For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Passphrase.

    a. Enter the password in the field provided. This is the password that the user has to provide to access to a URI that is tagged as requiring a passphrase for access. The minimum length for the password is 0 characters (or no password) with a maximum of 64 characters.

    b. Click the switch to green to **Mask Password**. When this feature is enabled, the password is hidden; otherwise, it converts to plain text.

    c. Type in the password again to confirm it and avoid an error on the page.

    ⓘ | **NOTE:** The **Confirm Password** field is invalid when the password displays as plain text.

    d. Set the **Active Time** (in minutes) that a password is active. The minimum amount is 1 minute and the maximum is 9999 minutes. The default duration is 60 minutes.

e. Input or edit the HTML for the **PassPhrase Page** field.

f. Click **Default** to reset the page to the default HTML code.

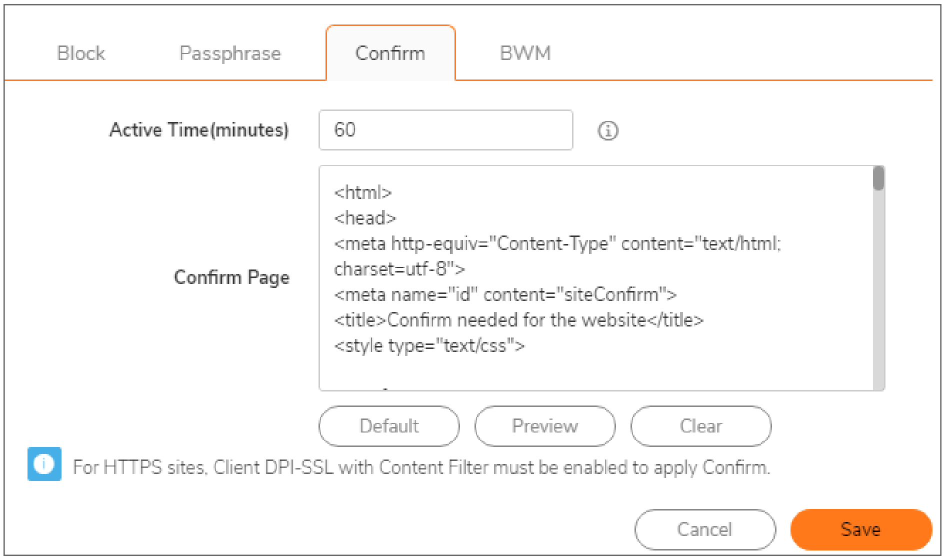
g. Click **Preview** see what is displayed when a URI is blocked.

h. Click **Clear** to clear the **Block Page** text block and start over.

i. Click **Save** to save the settings.

7. In the **Confirm** tab of the **Operations Configurations** section, define the settings for requiring a confirmation when certain URIs are detected.

   > ⓘ **NOTE:** For HTTPS sites, the Content Filtering option for the DPI-SSL Client SSL must be enabled to for **Confirm** to work. Navigate to the **General** tab at **POLICY | DPI-SSL > Client SSL** to set this.



Active Time(minutes): 60

Confirm Page:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
<meta name="id" content="siteConfirm">
<title>Confirm needed for the website</title>
<style type="text/css">
```

For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Confirm.

a. Set the **Active Time** (in minutes) during which the user must confirm their access to the URI.. The minimum amount is one minute and the maximum is 9999 minutes. The default duration is 60 minutes.

b. Input or edit the HTML for the **Confirm Page** field.

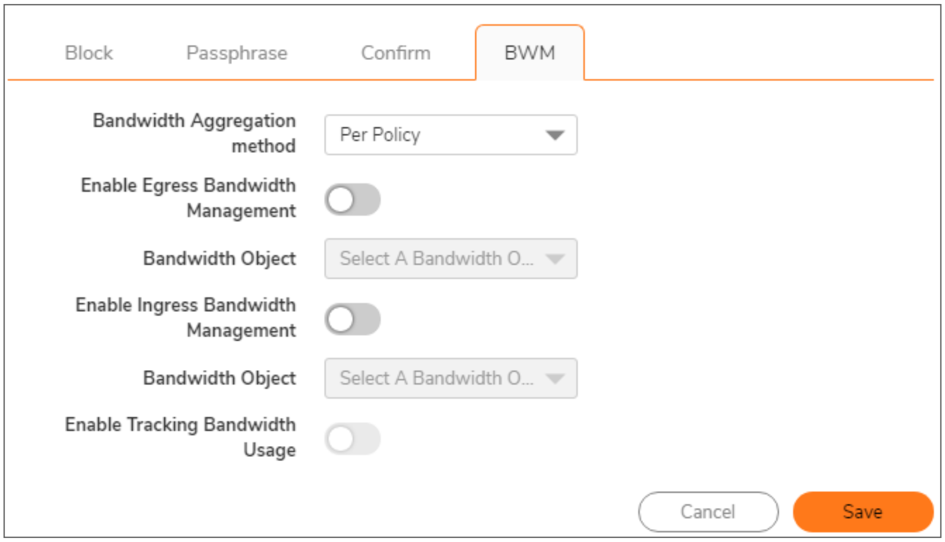
c. Click **Default** to reset the page to the default HTML code.

d. Click **Preview** see what is displayed when a URI is blocked.

e. Click **Clear** to clear the **Block Page** text block and start over.

f. Click **Save** to save the settings.

8. In the **BMW** tab of the **Operations Configurations** section, define the settings for bandwidth management when certain URIs are detected.



Bandwidth Aggregation method: Per Policy

Enable Egress Bandwidth Management: ○

Bandwidth Object: Select A Bandwidth O...

Enable Ingress Bandwidth Management: ○

Bandwidth Object: Select A Bandwidth O...

Enable Tracking Bandwidth Usage: ○

   a. Select a **Bandwidth Aggregation Method** from the drop-down menu.
   b. Click the switch to green to **Enable Egress Bandwidth Management**.
   c. Select the **Bandwidth Object** from the drop-down menu, or opt to create a new action object for egress bandwidth management.
   d. Click the switch to green to **Enable Ingress Bandwidth Management**.
   e. Select the **Bandwidth Object** from the drop-down menu, or opt to create a new action object for ingress bandwidth management.
   f. Click the switch to green to **Enable Tracking Bandwidth Management Usage**.
   g. Click **Save** to save the BMW settings.

Deleting Action Objects

Several different options are provided for deleting a Content Filtering Action Object. Whichever way you do it, you are asked to confirm that you really want to delete the item.

- You can select an individual action object by checking the box and clicking the **Delete** icon at the top or in the row you selected.
- You can simply highlight a row in the table and click the **Delete** icon at the end of the row you selected.
- You can select multiple action objects by checking the boxes and clicking the **Delete** icon at the top.

ⓘ | **NOTE:** The **CFS Default Action** cannot be deleted.

6

Configuring the Reputation Match Object

The Reputation match object is used to simplify the process for defining objects and policies. A reputation score is calculated and categorized based on value. The six categories are:

- High Risk
- Suspicious
- Moderate Risk
- Low Risk
- Trustworthy
- URL without Reputation

The Reputation Object defines the operation for something that is found to match one of these categories. Operations include Allow, Block, Confirm, Passphrase, and BWM. The default value for High Risk and Suspicious is to block access. The default for the other categories are to allow access.

SonicWall provided a CFS **Default Reputation Object.** This object cannot be deleted, but can be edited or cloned. Customized Reputation Objects can also be developed.

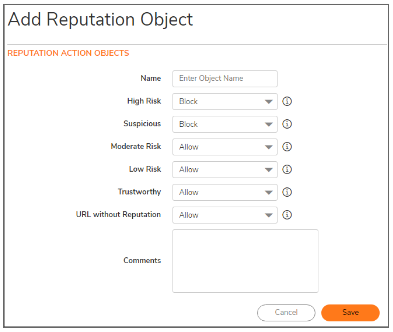
Topics:

- Adding or Editing a Reputation Object
- Cloning a Reputation Object
- Deleting a Reputation Object

Adding or Editing a Reputation Object

To add a Reputation Object:

1. Navigate to **OBJECT | Match Objects > Reputation**.
2. Click **+Add** to add a new object, or click the **Edit** icon for the object you want to edit.



Add Reputation Object

REPUTATION ACTION OBJECTS

Name	Enter Object Name
High Risk	Block
Suspicious	Block
Moderate Risk	Allow
Low Risk	Allow
Trustworthy	Allow
URL without Reputation	Allow
Comments	

3. Enter or update the object **Name**.
4. Select the action you want to take—**Allow**, **BMW**, **Block**, **Confirm**, or **Passphrase**—from the drop-down menu for each category. The categories are defined in the following table. The lower the scores indicate higher the risk.

Category	Reputation Score
High Risk	01-20
Suspicious	21-40
Moderate Risk	41-60
Low Risk	61-80
Trustworthy	81-100
URL without Reputation	0

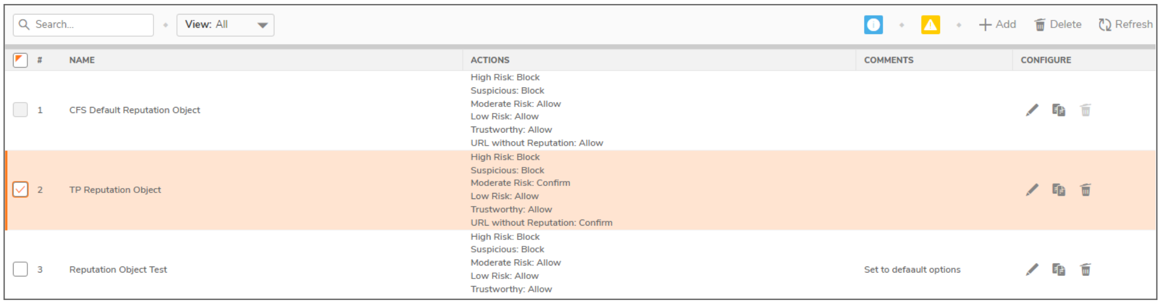
5. Add **Comments** in the field provided.
6. Click **Save**. The new object appears in the Reputation table.

Cloning a Reputation Object

The Cloning option allows you to copy an existing Reputation Object and customize it without having to start with a brand new, empty template. It is very similar to creating a new object, but you change only those fields that need to be different from the source.

To clone a Reputation Object:

1. Navigate to **OBJECT | Match Objects > Reputation**.
2. Select the object you want to clone.



☐	#	NAME	ACTIONS	COMMENTS	CONFIGURE
☐	1	CFS Default Reputation Object	High Risk: Block Suspicious: Block Moderate Risk: Allow Low Risk: Allow Trustworthy: Allow URL without Reputation: Allow		
☑	2	TP Reputation Object	High Risk: Block Suspicious: Block Moderate Risk: Confirm Low Risk: Allow Trustworthy: Allow URL without Reputation: Confirm		
☐	3	Reputation Object Test	High Risk: Block Suspicious: Block Moderate Risk: Allow Low Risk: Allow Trustworthy: Allow	Set to defaault options	

3. Select the **Clone** icon.
4. Give the object a new **Name**.
5. Change the category definitions as needed.
6. Add **Comments** in the field provided.
7. Click **Save**.

Deleting a Reputation Object

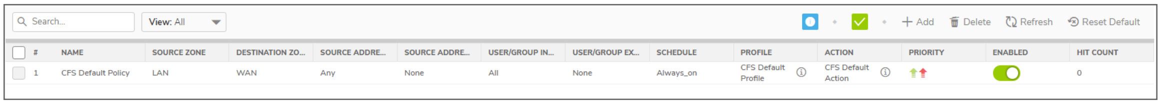
Several different options are provided for deleting a Content Filtering Reputation Object. However you do it, you are asked to confirm that you really want to delete the item.

- You can select an individual Reputation Object by checking the box and clicking the **Delete** icon at the top or in the row you selected.
- You can highlight a row in the table and click the **Delete** icon at the end of the row you selected.
- You can select multiple profile objects by checking the boxes and clicking the **Delete** icon at the top.

ⓘ | **NOTE:** The **CFS Default Reputation Object** cannot be deleted.

Configuring CFS Policies and Rules

After CFS is configured and the objects needed for the policy have been defined, you can define the CFS rules for managing CFS content. To define the CFS rules and policies, navigate to **POLICY | Rules and Policies > Content Filter Rules**.



□	#	NAME	SOURCE ZONE	DESTINATION ZO...	SOURCE ADDRE...	SOURCE ADDRE...	USER/GROUP IN...	USER/GROUP EX...	SCHEDULE	PROFILE	ACTION	PRIORITY	ENABLED	HIT COUNT
□	1	CFS Default Policy	LAN	WAN	Any	None	All	None	Always_on	CFS Default Profile	CFS Default Action	↑↑	●	0

Topics:

- Adding or Editing CFS Policy Rules
- Deleting CFS Policy Rules

Adding or Editing CFS Policy Rules

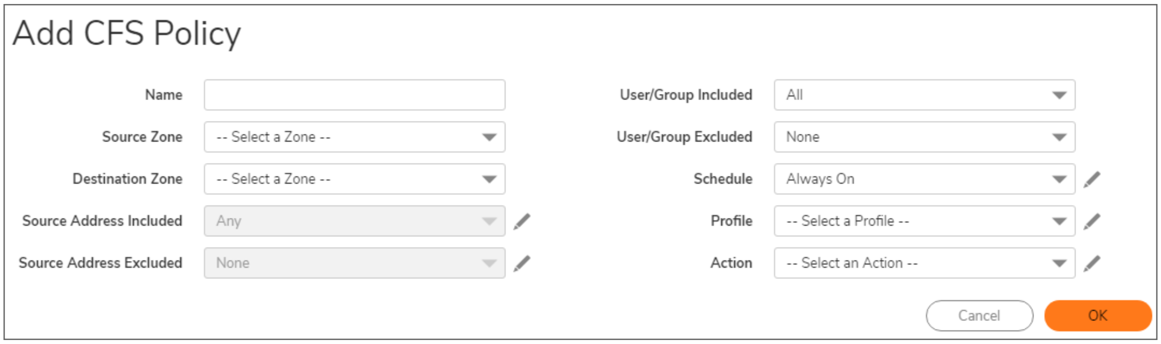
Adding and editing Content Filtering rules is very similar. The following procedures describe the options you can set in either instance.

To add a Content Filter Rule:

1. Navigate to **POLICY | Rules and Policies > Content Filter Rules**.
2. Click **+Add**.

To edit a Content Filer Rule:

1. Navigate to **POLICY | Rules and Policies > Content Filter Rules**.
2. Highlight the action object and click the **Edit** icon.



Add CFS Policy

Name		User/Group Included	All
Source Zone	-- Select a Zone --	User/Group Excluded	None
Destination Zone	-- Select a Zone --	Schedule	Always On
Source Address Included	Any	Profile	-- Select a Profile --
Source Address Excluded	None	Action	-- Select an Action --

To define or update the parameters for a Content Filer Rule:

1. Open the **CFS Policy** window as previously described.
2. Select a **Source Zone** from the drop-down menu.
3. Select a **Destination Zone** from the drop-down menu.
4. Select the **Source Address Included** from the drop-down menu. If you need to create a new address object for this rule, you can click the **Edit** icon beside the field.
5. Select the **Source Address Excluded** from the drop-down menu. If you need to create a new address object for this rule, you can click the **Edit** icon beside the field.
6. Select the **User/Group Included** from the drop-down menu.
7. Select the **User/Group Excluded** from the drop-down menu.
8. Select the **Schedule** from the drop-down menu during which the policy is applied. If you need to create a new schedule object for this rule, you can click the **Edit** icon beside the field.
9. Select the **Profile** from the drop-down menu. The items in the list are the same profiles listed in the CFS Profile Objects table at (missing or bad snippet). If you need to create a new profile object for this rule, you can click the **Edit** icon beside the field.
10. Select the **Action** from the drop-down menu. The items in the list are the same actions listed in the CFS Action Objects table at (missing or bad snippet). If you need to create a new action object for this rule, you can click the **Edit** icon beside the field.
11. Click **OK** when done.

Deleting CFS Policy Rules

Several different options are provided for deleting a Content Filtering policy and rules. Whichever way you do it, you are asked to confirm that you really want to delete the item.

- You can select an individual rule by checking the box and clicking the **Delete** icon at the top or in the row you selected.
- You can highlight a row in the table and click the **Delete** icon at the end of the row you selected.
- You can select multiple rules by checking the boxes and clicking the **Delete** icon at the top.

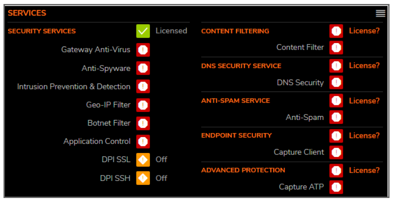
8

Monitoring Content Filtering

One of the first places you might look for status information is in the HOME section of the interface.

To confirm licensing status:

1. Navigate to **HOME | Dashboard > System > Device** tab.
2. Scroll down to see the **Services** pane.
3. Look for Content Filtering in that pane.



SERVICES

SECURITY SERVICES	✓	Licensed
Gateway Anti-Virus	!	
Anti-Spyware	!	
Intrusion Prevention & Detection	!	
Geo-IP Filter	!	
Botnet Filter	!	
Application Control	!	
DPI SSL	!	Off
DPI SSH	!	Off

CONTENT FILTERING	!	License?
Content Filter	!	
DNS SECURITY SERVICE	!	License?
DNS Security	!	
ANTI-SPAM SERVICE	!	License?
Anti-Spam	!	
ENDPOINT SECURITY	!	License?
Capture Client	!	
ADVANCED PROTECTION	!	License?
Capture ATP	!	

This example shows that Content Filtering Service is currently not licensed. You can click on the **License?** link to go to **DEVICE | Settings > Licenses** to renew or activate the suite of services with Content Filtering in it.

If your CFS license is active, you can also go to **HOME | Dashboard > System > Security Services** tab. Scroll to the Content Filter pane to see the details of the license.

9

SonicWall Support

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

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://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services at https://sonicwall.com/pes.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

SonicOS Content Filtering Administration Guide
Updated - December 2023
Software Version - 7.1
232-005886-00 Rev A

The information in this document is provided in connection with SonicWall 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 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 reserves the right to make changes to specifications and product descriptions at any time without notice. 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.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035