

SonicOS 7

Action Objects

Administration Guide

SONICWALL[®]

Contents

App Rule Actions	3
About Action Objects	4
About System Predefined Default Action Objects	4
About Action Types for Custom Action Objects	6
About Actions Using Bandwidth Management	7
Bandwidth Management Methods	9
Creating an Action Object	10
Modifying an Action Object	11
Related Tasks for Actions Using Packet Monitoring	11
Capturing Packets Related to a Policy	11
Configuring Mirroring	12
Content Filter Actions	14
About Content Filter Objects	14
About CFS Action Objects	15
About the Passphrase Feature	15
About the Confirm Feature	15
About UUIDs for CFS Objects	16
Managing CFS Action Objects	17
About the CFS Action Objects Table	17
Configuring CFS Action Objects	18
Editing CFS Action Objects	24
Deleting CFS Action Objects	25
Applying Content Filter Objects	25
SonicWall Support	26
About This Document	27

App Rule Actions

You can create a custom action object or select one of the predefined, default actions.

To view the action objects, navigate to **Object > Action Objects > App Rule Actions**.

#	NAME	ACTION TYPE	CONTENT
1	Advanced BWM High	Bandwidth Management	
2	Advanced BWM Low	Bandwidth Management	
3	Advanced BWM Medium	Bandwidth Management	
4	Block SMTP E-Mail Without Reply	Block SMTP E-Mail Without Reply	
5	Bypass Capture ATP	Bypass Capture ATP	
6	Bypass DPI	Bypass DPI	
7	Bypass GAV	Bypass GAV	
8	Bypass IPS	Bypass IPS	
9	Bypass SPY	Bypass SPY	
10	No Action	No Action	
11	Packet Monitor	Packet Monitor	
12	Reset/Drop	Reset/Drop	
13	FTP Server Read-only	FTP Notification Reply	This FTP server is read-only. Only an administrator can upload files.

Name	Name of the Action Object.
Action Type	Type of action provided by the Action Object, such as Bandwidth Management , Packet Monitor and so on.
Content	For Bandwidth Management Action Objects, displays a triangle icon. For user-configured Action Objects, displays the content provided in the Action Object Settings dialog.
Configure	<ul style="list-style-type: none"> • Edit icon: For system-provided Action Objects, the Edit icon is dimmed, and the Action Object cannot be modified. • Delete icon: For system-provided Action Objects, the Delete icon is dimmed, and the Action Object cannot be deleted.

Topics:

- [About Action Objects](#)
- [About Actions Using Bandwidth Management](#)
- [Creating an Action Object](#)
- [Modifying an Action Object](#)
- [Related Tasks for Actions Using Packet Monitoring](#)

About Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can create a custom action object or select one of the predefined, default actions.

Topics:

- [About System Predefined Default Action Objects](#)
- [About Action Types for Custom Action Objects](#)

About System Predefined Default Action Objects

There are a number of system defined, default actions that are predefined by SonicOS. These default action objects cannot be edited or deleted. The default actions are displayed in the **Add/Edit App Control Policy** dialog when you add or edit a policy from the **Policy > App Rules** page.

DEFAULT ACTION OBJECTS

The screenshot shows the 'Add App Rule' configuration window. On the left, there are fields for Policy Name, Policy Type (set to 'App Control Content'), Address Source, Address Destination, Service Source (set to 'Any'), Service Destination (set to 'SMTP (Send E-Mail)'), Exclusion Address, Match Object Included, Match Objects Excluded (set to 'None'), and Action Object (set to 'Reset/Drop'). On the right, there are fields for Users/Groups Included, Users/Groups Excluded, and Schedule. Below these are several toggle switches: 'Enable flow reporting' (off), 'Enable Logging' (on), 'Log individual object content' (off), 'Log using App Control message format' (on), and 'Log Redundancy Filter (seconds)' (on). There is also a 'Use Global Settings' field set to '1' and a 'Zone' dropdown. At the bottom right, there are 'Cancel' and 'OK' buttons.

A number of BWM action object options are available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **Object > Profile Objects > Bandwidth** page.

Several Bypass action options are available in the default action list. These are available if the indicated security services are licensed on the firewall.

See the below table for descriptions of the predefined action types. For more information about BWM actions, see [About Actions Using Bandwidth Management](#).

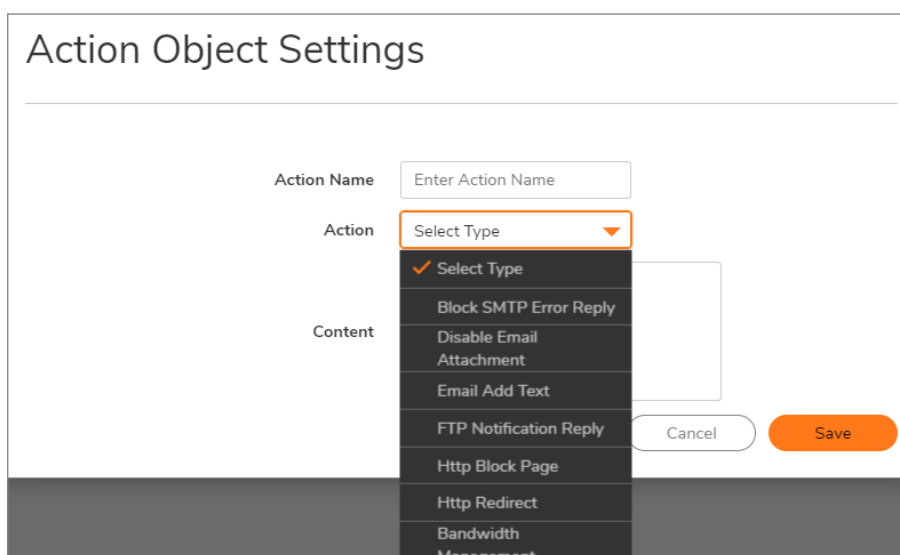
PREDEFINED DEFAULT ACTION OBJECT DESCRIPTIONS

Action Type	Description
Reset / Drop	For TCP, the connection will be reset. For UDP, the packet will be dropped.
No Action	Policies can be specified without any action. This allows “log only” policy types.
Bypass DPI	Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware and application control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel. Note that Bypass DPI does not stop filters that are enabled on the Network > Firewall > SSL Control page.
Packet Monitor	Use the SonicOS Packet Monitor capability to capture the inbound and outbound packets in the session, or if mirroring is configured, to copy the packets to another interface. The capture can be viewed and analyzed with Wireshark.
Advanced BWM High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of one.
Advanced BWM Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of four.
Advanced BWM Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of six.
Bypass GAV	Bypasses Gateway Anti-Virus inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.
Bypass IPS	Bypasses Intrusion Prevention Service inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.

Bypass SPY	Bypasses Anti-Spyware inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.
Bypass Capture ATP	Provides a way to skip Capture Advanced Threat Protection (ATP) analysis in specific cases when you know the file is free of malware. This action persists for the duration of the entire connection as soon as it is triggered. This option does not prevent other anti-threat components, such as GAV and Cloud Anti-Virus, from examining the file.

About Action Types for Custom Action Objects

The **Action** types available for creating custom action objects are displayed in the **Action Object Settings** dialog, which is displayed when you click **Add** at the top of the **Object > Action Objects > App Rule Actions** page.



Refer to the below table for descriptions of the action types.

① **NOTE:** You can create custom action objects in **Action Object Settings** dialog. The default predefined action objects cannot be edited or deleted. When you create a policy, the **Action Object Settings** dialog provides a way for you to select from the predefined action objects along with any custom actions that you have defined.

ACTION TYPES FOR CUSTOM ACTION OBJECTS

Action Type	Description
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.

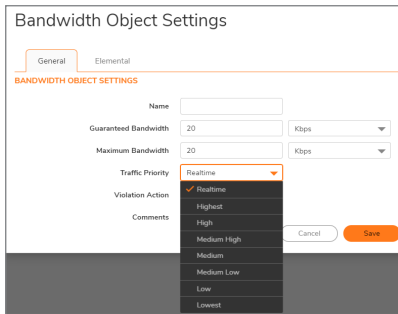
Email - Add Text	Appends custom text at the end of the email.
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: <i>http://www.google.com</i> . If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost.
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.

A priority setting of zero is the highest priority. Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

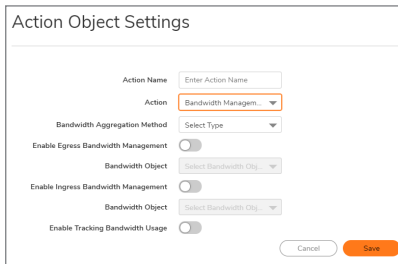
About Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For details about policy types, see **Policy > App Rules > Add App Rule** section.

As a best practice, configuring the global Bandwidth Management settings on the **Object > Profile Objects > Bandwidth** page should always be done before configuring any BWM policies.



ACTION OBJECTS PAGE WITH BANDWIDTH MANAGEMENT TYPE



Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. However, with App Rules you can specify all content type, which you cannot do with access rules.

For a bandwidth management use case, as an administrator you might want to limit .mp3 and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

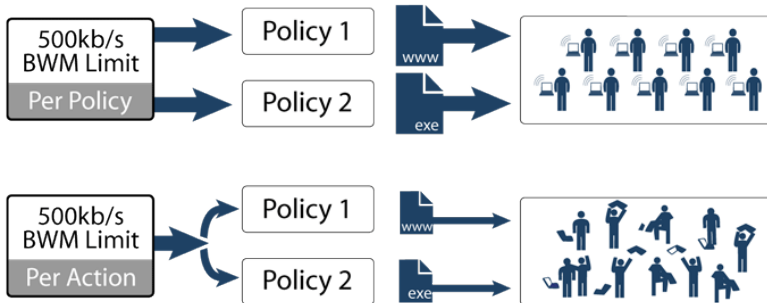
A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **Object > Profile Objects Bandwidth** page.

① | **NOTE:** Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

Bandwidth Management Methods

The Bandwidth Management feature can be implemented in two separate ways:

BANDWIDTH MANAGEMENT: IMPLEMENTATION METHODS



- Per Policy Method** – The bandwidth limit specified in a policy is applied individually to each policy. Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s.
- Per Action Aggregate Method** – The bandwidth limit action is applied (shared) across all policies to which it is applied. Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s.

The screenshot shows the 'Action Object Settings' dialog box. It includes fields for 'Action Name' (with a placeholder 'Enter Action Name'), 'Action' (set to 'Bandwidth Management'), 'Bandwidth Aggregation Method' (set to 'Per Action'), 'Enable Egress Bandwidth Management' (checked), 'Bandwidth Object' (set to 'Default Action Object BWM Egress High'), 'Enable Ingress Bandwidth Management' (unchecked), and 'Bandwidth Object' (set to 'Default Action Object BWM Ingress High'). There is also a checkbox for 'Enable Tracking Bandwidth Usage' which is currently unchecked. 'Cancel' and 'Save' buttons are at the bottom.

Displaying Bandwidth Management Action Object Information

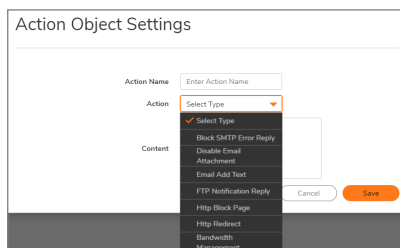
To display information about a Bandwidth Management Action Object, click on the triangle icon for the Action Object. The Bandwidth Management details are displayed.

#	NAME	ACTION TYPE	CONTENT
1	Advanced BWM High	Bandwidth Management	
<p style="text-align: center;">Aggregation Method Per Action</p> <p style="text-align: center;">Usage Tracking true</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>EGRESS PARAMETERS</p> <p>Egress Enabled</p> <p>Bandwidth Object Default Action Object BWM Egress High</p> <p>Per-IP Disabled</p> <p>Maximum</p> <p>Bandwidth Usage 0%</p> </div> <div style="width: 45%;"> <p>INGRESS PARAMETERS</p> <p>Ingress Enabled</p> <p>Bandwidth Object Default Action Object BWM Ingress High</p> <p>Per-IP Disabled</p> <p>Maximum</p> <p>Bandwidth Usage 0%</p> </div> </div>			

Creating an Action Object

SonicOS has a number of default predefined action objects, as described in [About System Predefined Default Action Objects](#). These action objects cannot be modified or deleted.

If you do not want one of the predefined actions, you can configure an Action Object. The **Action Object Settings** dialog, shown below, provides a way to customize a configurable action with text or a URL. You can select any of the action types available in the **Action** drop-down list. The predefined actions plus any configurable actions that you have created are available for selection when you create an App Rules policy.



To configure an Action Object:

1. Navigate to **Object > Action Objects > App Rule Actions**.
2. At the top of the page above the table, click **Add**.
3. In the **Action Object Settings** dialog, type a descriptive name in the **Action Name** field.
4. In the **Action** drop-down menu, select the action type that you want.
5. In the **Content** field, type the text or URL to be used in the action.
6. If **HTTP Block Page** was selected as the action type, the options change.
 - a. In the **Content** field, enter the content to be displayed when a page is blocked.
 - b. From the **Color** drop-down menu, choose a background color for the block page:
 - White
 - Yellow
 - Red
 - Blue
 - c. To preview the block page message, click the **Preview** button.
7. If **Bandwidth Management** was selected as the action type, the options change. For configuring these options, see [About Actions Using Bandwidth Management](#).
8. Click **OK**.

Modifying an Action Object

You can modify any custom Action Object you configure. System predefined default Action Objects cannot be modified.

To modify an Action Object:

1. Navigate to **Objects > Action Objects > App Rule Actions**.
2. Mouse over on the action object which you want to modify and click the **Edit** icon. The **Action Object Settings** dialog displays.
3. Follow **Step 3** through **Step 8** in **Modifying an Action Object** section.

Related Tasks for Actions Using Packet Monitoring

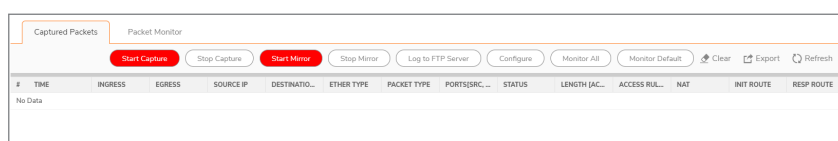
When the predefined Packet Monitor action is selected for a policy, SonicOS captures or mirrors the traffic according to the settings you have configured in the **Monitor > Tools & Monitors > Packets** page. The default is to create a capture file, which you can view with Wireshark™. For information about Wireshark, see **Policy > App Control** chapter.

After you have configured a policy with the Packet Monitor action, you still need to click **Start Capture** on the **Packets** page to actually capture any packets. After you have captured the desired packets, click **Stop Capture**.

Capturing Packets Related to a Policy

To control the Packet Monitor action to capture only the packets related to your policy:

1. Navigate to **Monitor > Tools & Monitors > Packets** page.



2. Click the **Configure** button.

3. In the **Packet Monitor Configuration** dialog, click **Monitor Filter**.

Packet Monitor Configuration

Settings | **Monitor Filter** | Display Filter | Logging | Advanced Monitor Filter | Mirror

MONITOR FILTER (USED FOR BOTH MIRRORING AND PACKET CAPTURE)

Enable filter based on the firewall/app rule ⓘ

Interface Name(s) ⓘ

Ether Type(s) ⓘ

IP Type(s) ⓘ

Source IP Address(es) ⓘ

Source Port(s) ⓘ

Destination IP Address(es) ⓘ

Destination Port(s) ⓘ

Enable Bidirectional Address and Port Matching ⓘ

Monitor

Forwarded packets only ⓘ

Consumed packets only

Dropped packets only

Default Cancel Save

4. Select **Enable Filter based on the firewall/app rule**. This option is not selected by default. In this mode, after you click **Start Capture** option on the **Capture Packets** page, packets are not captured until some traffic triggers the App Control policy (or an Access Rule). You can see the Alert message in the **Monitor > Logs > System Event** page when the policy is triggered. This works in App Rules policies created using an action object with Packet Monitor action type, or policies created in the **Policy > Access Rules** that use Packet Monitor, and allows you to specify configuration or filtering for what to capture or mirror. You can download the capture in different formats and look at it in a browser, for example.
5. Click **Save**.

Configuring Mirroring

To set up mirroring:

1. Navigate to **Monitor > Tools & Monitors > Packets** page.

Captured Packets | Packet Monitor

Start Capture Stop Capture Start Mirror Stop Mirror Log to FTP Server Configure Monitor All Monitor Default Clear Export Refresh

#	TIME	INGRESS	EGRESS	SOURCE IP	DESTINATIO..	ETHER TYPE	PACKET TYPE	PORT(S)SRC...	STATUS	LENGTH (AC...	ACCESS RUL...	NAT	INIT ROUTE	RESP ROUTE
No Data														

2. Click the **Configure** button.

3. In the **Packet Monitor Configuration** dialog, click **Mirror**.

The screenshot shows the 'Packet Monitor Configuration' dialog with the 'Mirror' tab selected. The dialog is divided into four sections: 'MIRROR SETTINGS', 'LOCAL MIRROR SETTINGS', 'REMOTE MIRROR SETTINGS (SENDER)', and 'REMOTE MIRROR SETTINGS (RECEIVER)'. At the bottom, there are 'Default', 'Cancel', and 'Save' buttons.

Section	Field Name	Value
MIRROR SETTINGS	Maximum mirror rate (in kilobits per second)	100
	Mirror only IP packets	Off
LOCAL MIRROR SETTINGS	Mirror filtered packets to Interface	None
REMOTE MIRROR SETTINGS (SENDER)	Mirror filtered packets to remote SonicWall firewall (IP Address)	0.0.0.0
REMOTE MIRROR SETTINGS (RECEIVER)	Receive mirrored packets from remote SonicWall firewall (IP Address)	0.0.0.0
	Send received remote mirrored packets to Interface	None
	Send received remote mirrored packets to capture buffer	Off

4. Pick an interface to which to send the mirrored traffic from the **Mirror filtered packets to Interface** drop-down menu under **Local Mirroring Settings**.
5. You can also configure one of the **Remote** settings. This allows you to mirror the application packets to another computer and store everything on the hard disk. For example, you could capture MSN Instant Messenger traffic and read the conversations.
6. Click **Save**.

Content Filter Actions

SonicWall Content Filtering Service (CFS) delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

① **NOTE:** For information about upgrading from an older version to CFS 4.0, see the *SonicWall Content Filtering Service Upgrade Guide*. Also, for applying these objects in CFS policies, see the *Policy > Security Services > Content Filter* section of *SonicOS Security Services*.

Topics:

- [About Content Filter Objects](#)
- [Managing CFS Action Objects](#)
- [Applying Content Filter Objects](#)

About Content Filter Objects

CFS uses secure objects for filtering content. For information about secure objects and their use, see the SonicOS Secure Objects section under *Network > Interfaces* in the *SonicOS System Setup* documentation. CFS uses the following objects for content filtering:

- CFS Action Objects – see [About CFS Action Objects](#)

You can add, edit, or delete any object except the **CFS Default Action** and **CFS Default Profile** objects created by SonicOS.

The Passphrase feature and Confirm (Consent) feature are also configured within content filter objects. The Passphrase feature restricts web access unless the user enters the correct passphrase or password. The Confirm feature restricts web access unless the user confirms that they want to proceed to the web site. See:

- [About the Passphrase Feature](#)
- [About the Confirm Feature](#)

SonicOS automatically generates and binds UUIDs (Universally Unique Identifiers) for all types of Content Filter objects during their creation. See [About UUIDs for CFS Objects](#) for more information.

About CFS Action Objects

The CFS Action Object defines what happens after a packet is filtered by CFS and matches a CFS policy.

About the Passphrase Feature

The Passphrase feature, in conjunction with the Confirm feature, restricts web access based on a passphrase or password. You can configure the passphrase operation for special URI categories or domains in the Forbidden URI List. To access the forbidden URIs, users are asked to enter the correct password or else web access is blocked.

① **IMPORTANT:** Passphrase only works for HTTP requests. HTTPS requests cannot be redirected to a Passphrase page.

For information about the Confirm feature, see [About the Confirm Feature](#).

How the Passphrase operation works:

1. The user attempts to access a restricted website.
2. A Passphrase page displays on the user's browser.
3. The user must enter the passphrase or password and then submit it.
4. CFS validates the submitted passphrase/password with the website's password:
 - If the passphrase/password matches, web access is allowed. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period set for the Confirm feature. The default is 60 minutes.
 - If the passphrase/password does not match, access is blocked, and a Block page is sent to the user.

① **NOTE:** Users have three chances to enter the passphrase/password. The site is blocked if all chances fail.

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

About the Confirm Feature

The Confirm feature (also known as Consent) restricts web access by requiring a confirmation from the user before allowing access. You can configure the Confirm operation for special URL categories or domains, and the users need to confirm the web request when they first visit the sites.

① **IMPORTANT:** Confirm only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm (Consent) page.

How the Confirm operation works:

1. The user attempts to access a blocked website.
2. A popup dialog appears, requesting confirmation.
3. Users must select **Continue** or **Close**.

- If a user confirms to access this category of websites, user is redirected to the first confirmed website. No further confirmations are needed, and users 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.
- If a user chooses **Close**, user is shown the Block page and is blocked from that category of website for the period of the Active Time setting.

About UUIDs for CFS Objects

SonicOS automatically generates and binds UUIDs (Universally Unique Identifiers) for these Content Filter objects and groups during their creation:

- URI List Object
- URI List Group
- CFS Action Object
- CFS Profile Object

SonicOS also generates and binds UUIDs to Content Filter Policies during creation. A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of an object and remains the same thereafter, even when the object is modified or after rebooting the firewall. The UUID is removed when the object is deleted and is not reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

By default, UUIDs are not displayed. UUID display is controlled by internal settings. For more information about internal settings, contact SonicWall Technical Support.

When displayed, UUIDs appear in the CFS object tables for each object or group type.

#	NAME	BLOCK	PASSPHRASE	CONFIRM	BWM	COMMENTS	UUID
1	CFS Default Action	✓	✓	✓	✓		35d4bc96-b6f8-3999-0d00-00401035094b

CFS object UUIDs facilitate the following functions:

- You can search for a CFS object by UUID with the global search function of the management interface.
- If an object with a UUID is referenced by another entity with a UUID, you can display the reference count and referring entity by mousing over the balloon on the CFS objects.

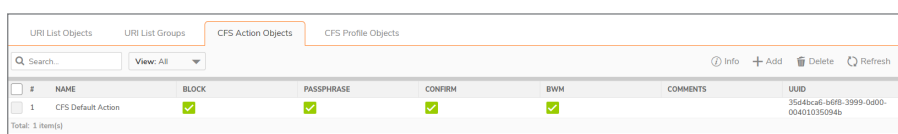
When a CFS Action Object, CFS Profile Object, URI List Object, or URI List Group is used by a Content Filter Policy, you can display the reference count and referenced policy by mousing over the balloon in the Comment column on the object's page under **Object**.

Managing CFS Action Objects

Topics:

- [About the CFS Action Objects Table](#)
- [Configuring CFS Action Objects](#)
- [Editing CFS Action Objects](#)
- [Deleting CFS Action Objects](#)

About the CFS Action Objects Table



The screenshot shows a management interface with four tabs: 'URI List Objects', 'URI List Groups', 'CFS Action Objects' (selected), and 'CFS Profile Objects'. Below the tabs is a search bar and a 'View: All' dropdown. The table has columns for '#', 'NAME', 'BLOCK', 'PASSPHRASE', 'CONFIRM', 'BWM', 'COMMENTS', and 'UUID'. A single row is visible with the following data: # 1, NAME CFS Default Action, BLOCK checked, PASSPHRASE checked, CONFIRM checked, BWM checked, COMMENTS, and UUID 35d4bc96-b6f8-3999-0d00-00401035094b. At the bottom left of the table, it says 'Total: 1 item(s)'.

Name	Name of the CFS Action Object; the name of the default CFS Action Object is CFS Default Action . The default object can be edited, but not deleted.
Block	Indicates whether a block page has been configured.
Passphrase	Indicates whether a passphrase page has been configured.
Confirm	Indicates whether a confirm page has been configured.
BWM	Indicates whether bandwidth management has been configured.
Comments	Contains comments added during the creation of CFS Action Objects.
UUID	Contains automatically generated UUIDs (Universally Unique Identifiers) for the Content Filter objects and groups.

Configuring CFS Action Objects

A default CFS Action Object, **CFS Default Action**, is created by SonicOS. You can configure and edit this CFS Action Object, but you cannot delete it.

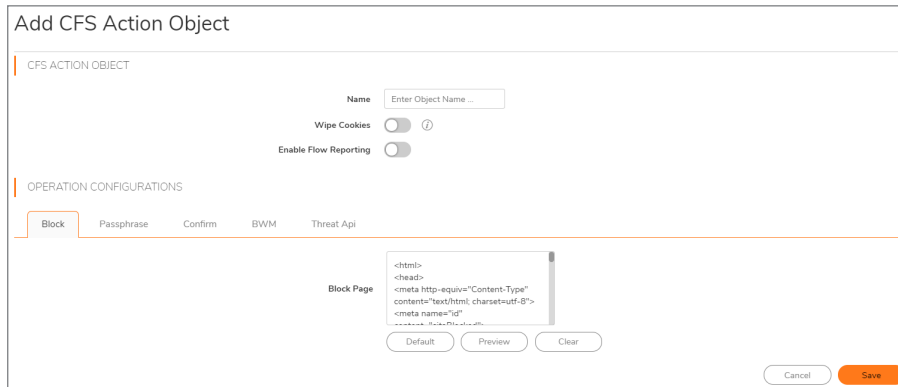
To configure CFS Action Objects:

1. Navigate to **Object > Action Objects > Content Filter Actions** page.
2. Click **Add** at the top of the page. The **Add CFS Action Object** dialog displays.

3. Enter the name of the CFS Action Object in the **Name** field.
4. To have cookies removed automatically to protect privacy, select the **Wipe Cookies** option. When enabled and Client DPI-SSL Content Filter is also enabled, cookies for HTTPS sites are removed. This option is not selected by default.
 - ① **IMPORTANT:** Enabling this option may break the Safe Search Enforcement function of some search engines.
5. To send URI information to the AppFlow Monitor, select the **Enable Flow Reporting** option. This option is not selected by default.
6. You can configure the following pages, which display when a site is blocked:
 - ① **NOTE:** A default version of each of these pages has been created. You can use the default, modify it to meet your needs, or create a new page.
 - Blocked site per company policy, go to [Block Option](#).
 - Password-protected web page, go to [Passphrase Option](#).
 - Restricted web page that requires confirmation before a user can view it, go to [Confirm Option](#).
 - Blocked site by Threat API enforcement, go to [Threat API Option](#).
7. You can allocate bandwidth resources as part of CFS Action Objects; go to [BWM Option](#).
8. Click **Save**. The new CFS Action Object is added to the CFS Action Object table.

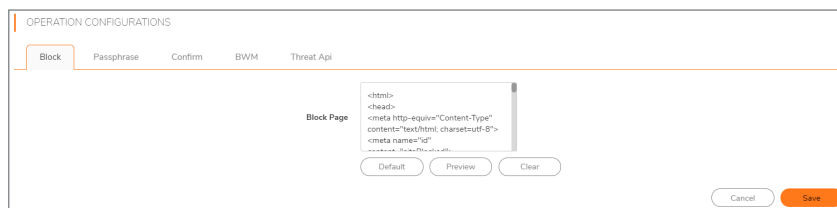
Block Option

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, navigate to **Object > Action Objects > Content Filter Actions** and click the **Add** button at the top of the page.



To create a page that displays when a site is blocked:

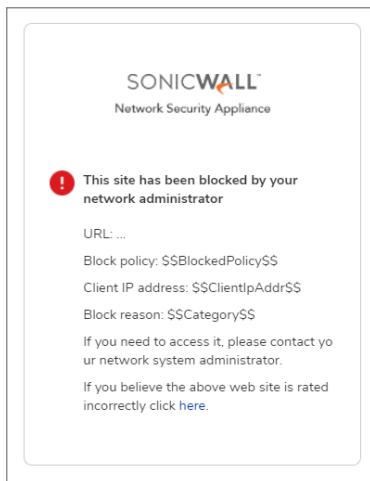
1. Under **Operation Configurations**, click the **Block** tab.



A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page.

2. To see a preview of the display, click the **Preview** button.
 3. If you have not modified the provided code, clicking the **Preview** button displays the default web page. The Block policy, Client IP address, and the reason for the block are shown.
- To remove all content from the Block Page field, click the **Clear** button.

To revert to the default blocked page message, click the **Default** button.



Passphrase Option

① | **NOTE:** For information about the Passphrase feature, see [About the Passphrase Feature](#).

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, navigate to **Object > Action Objects > Content Filter Actions** page and click the **Add** button at the top of the page.

To create a password-protected web page:

1. Under **Operation Configurations**, click the **Passphrase** tab.

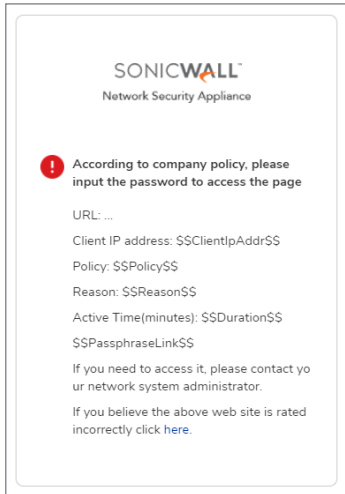
A screenshot of the "OPERATION CONFIGURATIONS" dialog box, specifically the "Passphrase" tab. The dialog has several tabs: "Block", "Passphrase", "Confirm", "BWM", and "Threat Api". The "Passphrase" tab is active. It contains the following fields and options: "Enter Password" (text input), "Mask Password" (toggle switch, currently on), "Confirm Password" (text input), "Active Time(minutes)" (text input, set to 60), and "PassPhrase Page" (text area containing HTML code). Below the text area are "Default", "Preview", and "Clear" buttons. At the bottom of the dialog, there is an "Informational" message: "For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Passphrase." and "Cancel" and "Save" buttons.

2. In the **Enter Password** field, enter the passphrase/password for the web site. The password can be up to 64 characters.
3. Enter it again in the **Confirm Password** field.
4. To have the password masked, select the **Mask Password** option. This option is selected by default.
① | **IMPORTANT:** If the option is deselected, the password is displayed in plain text and the entry in the **Confirm Password** field is invalid.
5. Enter the time, in minutes, of the effective duration for a passphrase based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.

6. A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:
 - To see a preview of the display, click the **Preview** button.
 - If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, policy, reason, and active minutes are shown along with a field for entering the password.

To remove all content from the Passphrase Page field, click the **Clear** button.

To revert to the default Passphrase page message, click the **Default** button.



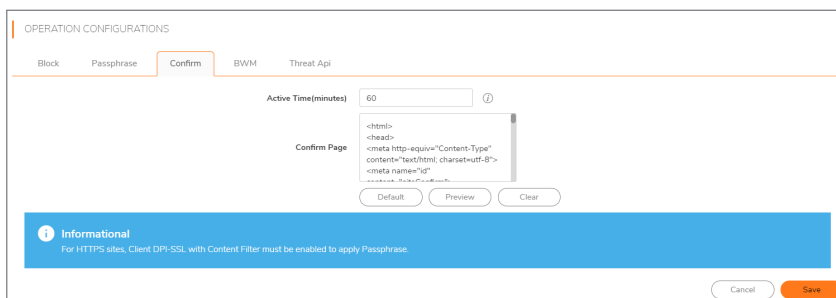
Confirm Option

NOTE: Requiring confirmation (consent) only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page. For more information, see [About the Confirm Feature](#).

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, navigate to **Object > Action Objects > Content Filter Actions** page and click the **Add** button at the top of the page.

To create a restricted web page that requires confirmation before a user can view it:

1. Under **Operation Configurations**, click the **Confirm** tab.

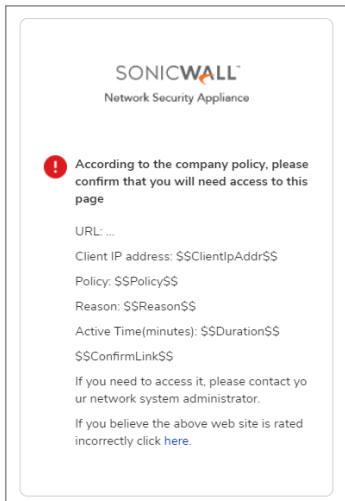


2. Enter the time, in minutes, of the effective duration for a confirmed user, based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.

3. A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a confirm site is attempted. Or, you can create your own page.
 - To see a preview of the display, click the **Preview** button.
 - If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation.

To remove all content from the Confirm Page field, click the **Clear** button.

To revert to the default blocked page message, click the **Default** button.



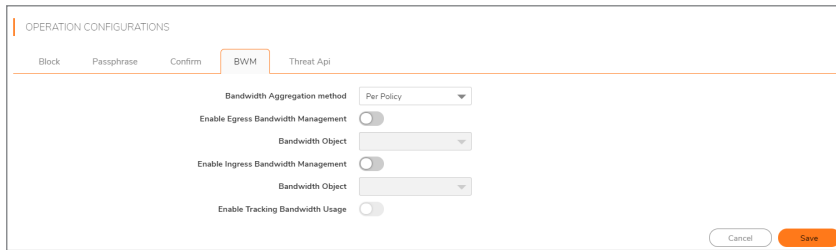
BWM Option

- ① **IMPORTANT:** CFS Action bandwidth Objects are similar to, but not the same as, bandwidth objects created on the **Object > Profile Objects > Bandwidth** page. CFS Action BWM objects do not appear on the **Object > Profile Objects > Bandwidth** page, and BWM bandwidth objects do not appear on the **Object > Action Objects > Content Filter Actions** page.
- ① **NOTE:** For information about bandwidth management, see the [About Actions Using Bandwidth Management](#).
- ① **IMPORTANT:** To create a CFS Action BWM object, Bandwidth Management must be enabled.

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, navigate to **Object > Action Objects > Content Filter Actions** page and click the **Add** button at the top of the page.

To allocate bandwidth resources for content filtering:

1. Under **Operation Configurations**, click the **BWM** tab.



2. From the **Bandwidth Aggregation Method** drop-down menu, choose how the BWM object is to be applied:
 - Per Policy (default)
 - Per Action
3. To enable BWM on outbound traffic, select the **Enable Egress Bandwidth Management** option. This option is not selected by default. The **Bandwidth Object** drop-down menu and the **Enable Tracking Bandwidth Usage** option become active.
 - a. From the **Bandwidth Object** drop-down menu, choose either:
 - An existing BWM object.
 - Create new Bandwidth Object. The Add Bandwidth Object dialog displays. For information on creating a new bandwidth object, see **Object > Profile Objects > Bandwidth** chapter.
4. To enable BWM on inbound traffic, select the **Enable Ingress Bandwidth Management** option. This option is not selected by default. The **Bandwidth Object** drop-down menu becomes active.
 - a. From the **Bandwidth Object** drop-down menu, choose either:
 - An existing BWM object.
 - Create new Bandwidth Object. The Add Bandwidth Object dialog displays. For information on creating a new bandwidth object, see **Object > Profile Objects > Bandwidth** chapter.
5. To track bandwidth usage, select the **Enable Tracking Bandwidth Usage** option. This option is not selected by default.

① **NOTE:** Enable Egress Bandwidth Management and/or Enable Ingress Bandwidth Management must be selected to activate the Enable Tracking Bandwidth Usage option.

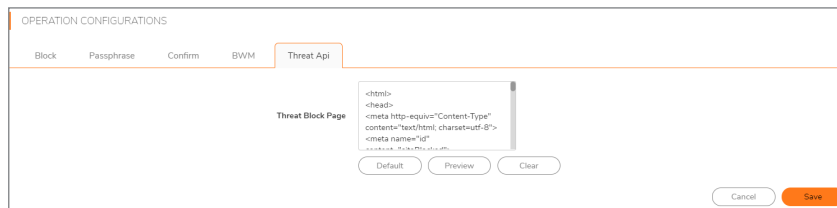
Threat API Option

① | **IMPORTANT:** Before configuring Threat API, you must enable it.

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, navigate to **Object > Action Objects > Content Filter Actions** page and click the **Add** button at the top of the page.

To add a policy to block URLs in the threat list:

1. Under **Operation Configurations**, click the **Threat API** tab.

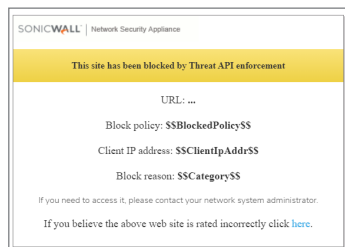


2. A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:

- To see a preview of the display, click the **Preview** button.
- If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation:

To remove all content from the Confirm Page field, click the **Clear** button.

To revert to the default confirm page message, click the **Default** button.



Editing CFS Action Objects

To edit a CFS Action Object:

1. Navigate to **Object > Action Objects > Content Filter Actions** tab.
2. Mouse over and click the **Edit** icon for the CFS Action Object to be edited. The **Edit CFS Action Object** dialog displays. This dialog is the same as the **Add CFS Action Object** dialog.
3. To make your changes, follow the appropriate procedures in [Configuring CFS Action Objects](#).

Deleting CFS Action Objects

To delete CFS Action Objects:

1. Navigate to **Object > Action Objects > Content Filter Actions** page.
2. Do one of the following:
 - Mouse over on the action object and click the **Delete** icon.
 - Click the checkbox for one or more action objects to be deleted. Click the **Delete** button.

Applying Content Filter Objects

After you finish configuring your Content Filter Objects, you need to apply them to Content Filter policies. Configuring Content Filters is done on the **Policy > Security Services > Content Filter** page (see the *Configuring Content Filtering Service* section of *SonicOS Security Services*).

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
- 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

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **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.

SonicOS Action Objects Administration Guide

Updated - February 2021

Software Version - 7

232-005323-10 Rev A

Copyright © 2021 SonicWall Inc. All rights reserved.

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