



SonicOS 7

Security Services

Administration Guide

SONICWALL®

# Contents

<b>Summary</b> .....	<b>5</b>
Synchronize Licenses .....	5
Security Services Settings .....	5
Signature Downloads Through a Proxy Server .....	6
Security Services Information .....	6
<b>Configuring Content Filter</b> .....	<b>8</b>
SonicWall CFS .....	8
CFS Status .....	9
Global Settings .....	9
CFS Exclusion .....	9
CFS Custom Category .....	10
Websense Enterprise .....	10
Websense Server Status .....	10
General Settings .....	10
Block Web Features .....	10
CFS Exclusion .....	11
Blocking Page .....	11
<b>Managing the SonicWall Gateway Anti-Virus Service</b> .....	<b>12</b>
SonicWall GAV Multi-Layered Approach .....	13
Remote Site Protection .....	13
Internal Network Protection .....	14
HTTP File Downloads .....	14
Server Protection .....	14
Cloud Anti-Virus Database .....	15
SonicWall GAV Architecture .....	15
Activating the Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention License .....	16
Setting Up SonicWall Gateway Anti-Virus Protection .....	16
Viewing SonicWall Gateway Anti-Virus Status Information .....	17
Enabling SonicWall Gateway Anti-Virus .....	18
Applying SonicWall Gateway Anti-Virus Protection on Zones .....	18
Specifying Protocol Filtering .....	18
Configuring Gateway Anti-Virus Settings .....	20
Configuring Cloud Gateway Anti-Virus .....	22
Viewing SonicWall Gateway Anti-Virus Signatures .....	23
Displaying Signatures .....	23
Navigating the Gateway Anti-Virus Signatures Table .....	24
Searching the Gateway Anti-Virus Signature Database .....	24

<b>Anti-Spyware Service</b> .....	<b>25</b>
Anti-Spyware Status .....	25
Anti-Spyware Global Settings .....	26
Signature Groups .....	26
Protocols .....	27
Anti-Spyware Signatures .....	27
<b>Intrusion Prevention Service</b> .....	<b>28</b>
About Intrusion Prevention Service .....	28
Enabling Intrusion Prevention Services .....	30
IPS Status .....	30
IPS Global Settings .....	30
Intrusion Prevention Service Policies .....	31
<b>Configuring Geo-IP Filters</b> .....	<b>32</b>
Configuring Geo-IP Filtering .....	32
Creating Custom Country Lists .....	34
Customizing Web Block Page Settings .....	34
Using Geo-IP Filter Diagnostics .....	35
Geo-IP Cache Statistics .....	35
Custom Countries Statistics .....	35
Show Resolved Locations .....	36
Check GEO Location Server Lookup .....	36
Incorrectly Marked Address .....	36
<b>Configuring Botnet Filters</b> .....	<b>37</b>
Configuring Botnet Filtering .....	37
Creating Custom Botnet Lists .....	38
Creating a Custom Botnet List .....	39
Editing Custom Botnet List Entries .....	39
Editing Custom Botnet List Entries .....	40
Configuring Dynamic HTTP Authentication .....	40
Customizing Web Block Page Settings .....	41
Using Botnet Filter Diagnostics .....	41
Botnet Cache Statistics .....	42
Botnets Statistics .....	42
Show Resolved Botnet Locations .....	42
Check Botnet Server Lookup .....	42
Incorrectly Marked Address .....	43
Displaying the Status of the Botnet Feature and Database .....	43
<b>Configuring App Control</b> .....	<b>44</b>
About App Control Policy Creation .....	45
Viewing App Control Status .....	45
Enabling App Control .....	46

Enabling App Control Globally .....	46
Enabling App Control on Zones .....	46
Configuring Logging and Log Filter Interval .....	47
Enabling App Control Filename Logging .....	48
Configuring App Control Global Settings .....	48
About App Control Global Settings .....	49
Configuring App Control Advanced Settings .....	50
Configuring App Control Advanced by Category .....	50
Configuring App Control Advanced by Application .....	52
Configuring App Control Advanced by Signature .....	54
Viewing Signatures .....	56
<b>SonicWall Support .....</b>	<b>62</b>
About This Document .....	63

# Summary

This feature allows SonicWall network security appliances that operate in networks to access the Internet through a proxy server to download signatures. This feature also allows for registration of SonicWall network security appliances through a proxy server to avoid compromising privacy.

The **Security Services > Summary** page provides these settings:

- [Synchronize Licenses](#)
- [Security Services Settings](#)
- [Signature Downloads Through a Proxy Server](#)
- [Security Services Information](#)

These top-level **Security Services** settings allow a choice of operating for maximum security, or accepting less than the highest security level but with higher network performance levels.

These settings can be selected for the global network, a group, or a single SonicWall network security appliance.

## Synchronize Licenses

To synchronize your licenses with your [MySonicWall](#) account, click the **Synchronize** button in the **Synchronize Licenses** section.

## Security Services Settings

The Security Services Settings includes these settings:

- **Security Services Setting**

There are two choices of security levels:

- **Maximum Security (Recommended)** — This setting results in the inspection of all traffic, regardless of the threat level.
  - **Performance Optimized** — This setting restricts inspection to traffic having a high or medium threat level. It speeds up throughput at the expense of the highest level of security
- SonicOS DPI clustering allows additional performance in the maximum security setting.

- **Reduce Anti-Virus traffic for ISDN connections** — With this setting enabled, SonicWall Anti-Virus checks for updates only once a day (every 24 hours), thereby reducing the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Drop all packets while IPS, GAV and Anti-Spyware database is reloading** — Select this option to instruct the SonicWall network security appliance to drop all packets whenever the IPS, GAV, and Anti-Spyware database is updating.
- **HTTP Clientless Notification Timeout for Gateway AntiVirus and Ant-Spyware** — HTTP Clientless Notification notifies users when an incoming threat from an HTTP server is detected. Set the timeout duration, in seconds, after which the SonicWall network security appliance notifies users when Gateway Anti-Virus or Anti-Spyware detects an incoming threat from an HTTP server. The default timeout is one day (86400 seconds), the minimum time is 10 seconds, and the maximum time is 2147483647 seconds. This defines the length of time the appliance waits for a confirmation notification from a client system.

## Signature Downloads Through a Proxy Server

Setting up a proxy server is essential as a method for maintaining privacy for downloading threat signatures and appliance registration.

*To enable signature download or appliance registration through a proxy server:*

1. Select **Download Signatures through a Proxy Server**.
2. If this field is selected, the next two fields become available. In the **Proxy Server Name or IP Address** field, enter the hostname or IP address of the proxy server.
3. In the **Proxy Server Port** field, enter the port number used to connect to the proxy server.
4. Select **This Proxy Server requires Authentication** if the proxy server requires a username and password.
  - ① **NOTE:** If you leave the password field empty, the current password value for this appliance remains unchanged.
5. Click **Accept** to apply the changes or **Cancel** to discard the changes.

## Security Services Information

The **Import Signature** feature available in this section is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons). The **Import Signature** feature provides a method to update the latest signatures at your discretion:

1. Download the signatures from your **MySonicWall** account to a separate computer, a USB drive, or other media.
2. Upload the signatures to the firewall.

The same signature update file can be used on all SonicWall network security appliances that meet these requirements:

- Devices that are registered to the same **MySonicWall** account
- Devices that belong to the same class of SonicWall network security appliances.

**To manually update signature files:**

1. Navigate to the **Security Services > Summary**.
2. Scroll to the **Security Services Information** section (at the bottom of the page).
3. Record the **Signature File ID** for the device.
4. Log on to **MySonicWall** account that was used to register the SonicWall network security appliance.  
① | **NOTE:** The signature file can only be used on network security appliances that are registered to the MySonicWall account that downloaded the signature file.
5. Navigate to **Resources & Support > Download Center**.
6. Click on **Download Signatures**.
7. In the pull down window next to Signature ID:, select the appropriate SFID for your firewall.
8. Download the signature update file by clicking on **Click here to download the Signature file**.  
① | **NOTE:** The remaining steps can be performed while disconnected from the Internet.
9. Return to the Security Services > Summary page on the network security appliance management interface.
10. Next to **Import Signatures**, click the **Import** button.
11. When the file dialog displays, navigate to the location of the signature update file.
12. Click **Open**. The signatures are uploaded for the security services that are enabled on the firewall.
13. Click **Accept**.

# Configuring Content Filter

The **Content Filter** page provides a list of the filtering types and gives the link to the pages for finding SonicWall CFS objects and policies. Click on the **Content Filtering Type** to select the content filtering options you want to view:

Content Filtering Type	Description
<b>SonicWall CFS</b>	SonicWall CFS is the standard content filtering service.
<b>Websense Enterprise</b>	Websense Enterprise is an enhancement of the SonicWall Content Filtering Service. It allows organizations that have deployed a joint SonicWall and Websense Enterprise solution to enforce web access policies on HTTPS connections.

## Topics:

- [SonicWall CFS](#)
- [CFS Custom Category](#)
- [Websense Enterprise](#)

## SonicWall CFS

This section allows the administrator to configure client Content Filtering Service (CFS) settings in SonicOS. The default SonicWall Content Filtering Service policy is available without a CFS subscription. With a valid advanced CFS subscription, you can create custom CFS policies and apply them to network zones or to groups of users within your organization.

The main settings for the SonicWall CFS policy are configured on these pages:

- You can access all the CFS Policies from the **POLICY | Rules and Policies > Content Filter Rules** page.
- You can access all the CFS Objects from the **OBJECT | Match Objects > Content Filter/URL** page.

After you have configured a CFS policy, you can configure client content filtering settings.

SonicOS offers client content filtering protection on a subscription-basis through a partnership with McAfee.



## Topics:

- [CFS Status](#)
- [Global Settings](#)
- [CFS Exclusion](#)

## CFS Status

The **CFS Status** section displays the current licensing status, license expiration date, and CFS server availability.

## Global Settings

The **Global Settings** section of the **Content Filter** page brings up the information for defining the global settings for CFS policies. Many of the fields on this page have an *i* (information) icon on the right, which gives more information about that field. The **Global Settings** section provides these configuration options:

<b>Max URL Cache Entries</b>	You can select the maximum number of URL entries that can be cached. The minimum is 25,600 and the maximum is 51,200. In the note beneath this field, there is a link on the word “here” that gives the supported range for the selected model.
<b>Enable Content Filtering Service</b>	This setting defaults to <b>Enabled</b> .
<b>Block if CFS Server is Unavailable</b>	When this option is selected, if the CFS server is detected as unavailable, then all web access is blocked.
<b>Server Timeout</b>	If the network security appliance does not get a response from the CFS server within this timeout value, the sever is marked as unavailable. The minimum is two seconds, the maximum is 10 seconds, and the default is five seconds. This setting is not available when <b>Block if CFS Server is Unavailable</b> is not checked.
<b>Enable Local CPS Server</b>	Check this box for the local CFS server. This setting defaults to disabled.
<b>Primary Local CFS Server</b>	This field holds the IP address for primary local CFS server. It becomes available when <b>Enable Local CFS Server</b> is checked.
<b>Secondary Local CFS Server</b>	This field holds the IP address for secondary local CFS server. It becomes available when <b>Enable Local CFS Server</b> is checked.

## CFS Exclusion

The options in the **CFS Exclusion** section can be configured to allow packets from the administrator and a number of address objects to pass through unfiltered.

<b>Exclude Administrator</b>	All the packets from the administrator pass through the CFS module if this box is checked. It defaults to enabled.
<b>Excluded Address</b>	Select addresses from the list, as desired. The packets of all selected

## CFS Custom Category

The **CFS Custom Category** section allows the configuration of new custom CFS category entries. The administrator can create custom policies and categories, and insert the domain name entries into the existing, flexible CFS rating category structure. Categories are added and deleted on the page that follows:

- Click **Add** to bring up a dialog box where you can choose from a list of categories to add to the CFS categories in your system. Choose the Domain name and the categories, then click **OK** to add them.
- Click **Update** on the **Content Filter** page to save your changes. If changes have been made, clicking **Update** opens a dialog box to select a schedule for the application and persistence of your changes.

## Websense Enterprise

The **Websense Enterprise** option on the **Content Filter Type** field brings up the page for configuring Websense Enterprise settings.


### Topics:

- [Websense Server Status](#)
- [General Settings](#)
- [Block Web Features](#)
- [CFS Exclusion](#)
- [Blocking Page](#)

## Websense Server Status

The **Websense Server Status** section displays the current licensing status, license expiration date, and CFS server availability.

## General Settings

The **General Settings** section is where basic information about the Websense Server can be set. Click the  icon to bring up the screen tips that guide the user in making the choices for these fields.

When **Enable Websense Probe Monitoring** is enabled, options become available for controlling the probing operation.

## Block Web Features

The **Block Web Features** section sets the blocking system for features and domains, as selected by the administrator.

## CFS Exclusion

The options in the **CFS Exclusion** section can be configured to allow packets from the administrator and a number of address objects to pass through unfiltered.

---

<b>Exclude Administrator</b>	All the packets from the administrator pass through the CFS module if this box is checked. It defaults to enabled.
<b>Excluded Address</b>	Select addresses from the list, as desired. The packets of all selected addresses pass through the CFS module.

---

## Blocking Page

The **Blocking Page** section allows you to customize the message displayed by the Websense Enterprise server when a message is blocked.

# Managing the SonicWall Gateway Anti-Virus Service

SonicWall Gateway Anti-Virus (GAV) service delivers real-time virus protection directly on the SonicWall network security appliance by using SonicWall's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWall gateway. Building on SonicWall's reassembly-free architecture, SonicWall GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWall GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWallGAV delivers threat protection by matching downloaded or emailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWall's SonicAlert Team, third-party virus analysts, open source developers, and other sources.

SonicWall GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications, and dozens of other stream-based protocols, to provide you with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWall GAV integrates advanced decompression technology that automatically decompresses and scans files on a per-packet basis.

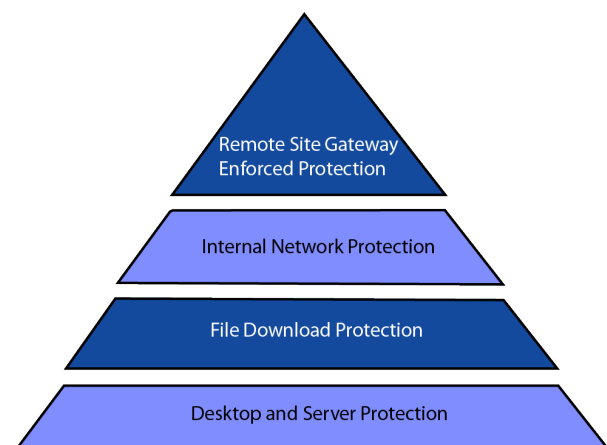
SonicWall GAV parses supported email protocols for the header fields To, CC, and BCC. The information in these fields are displayed and logged in Capture ATP for both sender and receiver.

## Topics:

- [SonicWall GAV Multi-Layered Approach](#)
- [SonicWall GAV Architecture](#)
- [Activating the Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention License](#)
- [Setting Up SonicWall Gateway Anti-Virus Protection](#)
- [Viewing SonicWall Gateway Anti-Virus Signatures](#)

# SonicWall GAV Multi-Layered Approach

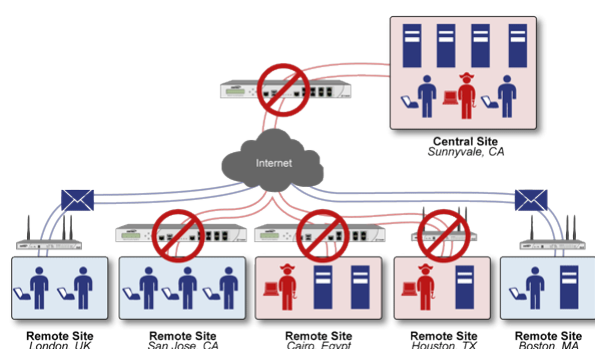
SonicWall Gateway Anti-Virus delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites; see SonicWall GAV multi-layer approach. SonicWall GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.



## Topics:

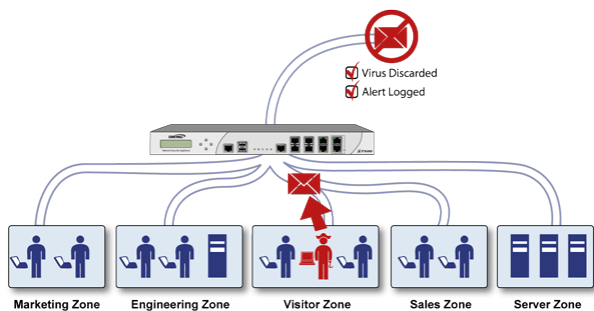
- [Remote Site Protection](#)
- [Internal Network Protection](#)
- [HTTP File Downloads](#)
- [Server Protection](#)
- [Cloud Anti-Virus Database](#)

## Remote Site Protection



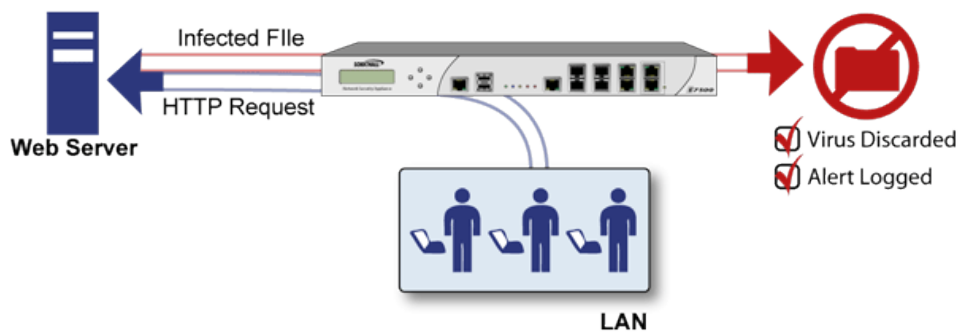
1. Users send typical e-mail and files between remote sites and the corporate office.
2. SonicWall GAV scans and analyzes files and e-mail messages on the SonicWall network security appliance.
3. Viruses are found and blocked before infecting remote desktop.
4. The virus is logged, and an alert is sent to the administrator.

# Internal Network Protection



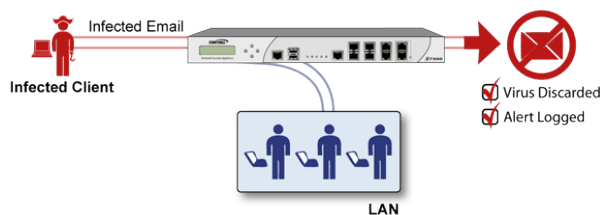
1. Internal user contracts a virus and releases it internally.
2. All files are scanned at the gateway before being received by other network users.
3. If a virus is found, the file is discarded.
4. The virus is logged, and an alert is sent to the administrator.

# HTTP File Downloads



1. Client makes a request to download a file from the Web.
2. The file is downloaded through the Internet.
3. The file is analyzed the SonicWall GAV engine for malicious code and viruses.
4. If a virus is found, the file is discarded.
5. The virus is logged, and an alert is sent to the administrator.

# Server Protection



1. Outside user sends an incoming email.
2. The email is analyzed by the SonicWall GAV engine for malicious code and viruses before being received by the email server.
3. If a virus is found, the threat is prevented.
4. The email is returned to the sender, the virus is logged, and an alert sent to the administrator.

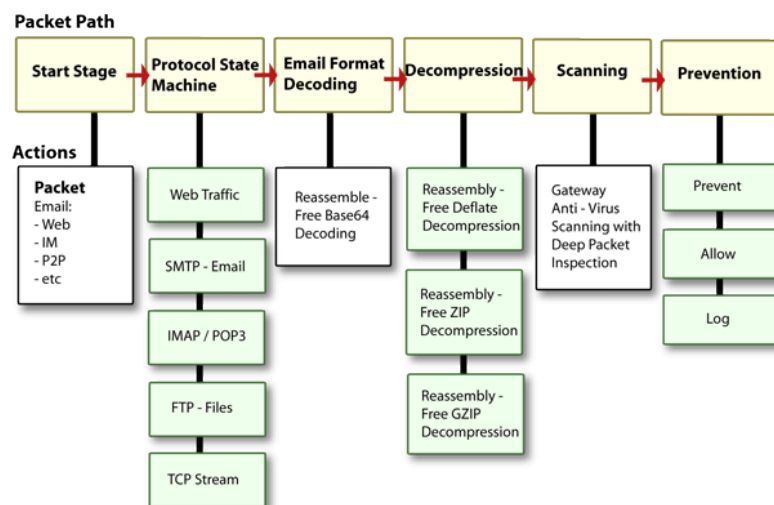
## Cloud Anti-Virus Database

The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway Anti-Virus scanning mechanisms present on SonicWall network security appliances to counter the continued growth in the number of malware samples in the wild.

Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection (RFDPI) engine capabilities by consulting with the datacenter-based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, SonicWall's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

## SonicWall GAV Architecture

SonicWall Gateway Anti-Virus (GAV) is based on SonicWall's high performance Deep Packet Inspection version 2.0 engine (DPIv2.0) engine, which performs all scanning directly on the SonicWall security appliance. SonicWall GAV includes advanced decompression technology that can automatically decompress and scan files on a per-packet basis to search for viruses and malware. The SonicWall GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWall GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWall GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.



Building on SonicWall's reassembly-free architecture, SonicWall GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWall GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWall GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

① **TIP:** If your SonicWall network security appliance is connected to the Internet and registered at mySonicWall.com, you can activate a 30-day FREE TRIAL of SonicWall Gateway Anti-Virus, SonicWall Anti-Virus, and SonicWall Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

## Activating the Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention License

Your network security appliance must be registered on [MySonicWall](#) to use these security services. See your *Quick Start Guide* for information on creating a [MySonicWall](#) account and registering your appliance. For information about upgrading the services in a closed environment, see *SonicWall SonicOS 7 Upgrade Guide*.

Because SonicWall Anti-Spyware is part of SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention, the Activation Key you receive is for all three services on your SonicWall network security appliance.

If you do not have a SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention. license activated on your SonicWall network security appliance, you must purchase it from a SonicWall reseller or through your [MySonicWall](#) account (limited to customers in the USA and Canada).

### Activating FREE TRIAL Versions

You can try FREE TRIAL versions of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention. For information about activating a free trial of any or all of the Security Services, see the *Quick Start Guide* for your appliance.

## Setting Up SonicWall Gateway Anti-Virus Protection

Activating the SonicWall Gateway Anti-Virus license on your SonicWall network security appliance does not automatically enable the protection.

### To configure SonicWall Gateway Anti-Virus:

1. Enable SonicWall Gateway Anti-Virus.
2. Apply SonicWall Gateway Anti-Virus Protection to zones.



## Topics:

- [Viewing SonicWall Gateway Anti-Virus Status Information](#)
- [Enabling SonicWall Gateway Anti-Virus](#)
- [Applying SonicWall Gateway Anti-Virus Protection on Zones](#)
- [Specifying Protocol Filtering](#)
- [Configuring Cloud Gateway Anti-Virus](#)

# Viewing SonicWall Gateway Anti-Virus Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWall signature servers were last checked for the most current database version. The SonicWall network security appliance automatically attempts to synchronize the database on startup, and once every hour.

## Topics:

- [Checking the SonicWall Gateway Anti-Virus Signature Database Status](#)
- [Updating SonicWall Gateway Anti-Virus Signatures](#)

# Checking the SonicWall Gateway Anti-Virus Signature Database Status

The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp** displays the last update to the SonicWall Gateway Anti-Virus signature database, not the last update to your SonicWall network security appliance.
- **Last Checked** indicates the last time the SonicWall network security appliance checked the signature database for updates. The SonicWall network security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWall Gateway Anti-Virus service expires. If your SonicWall Gateway Anti-Virus subscription expires, the SonicWall IPS inspection is stopped and the SonicWall Gateway Anti-Virus configuration settings are removed from the SonicWall network security appliance. These settings are automatically restored after renewing your SonicWall Gateway Anti-Virus license to the previously configured state.
- The **Gateway Anti-Virus** section displays **Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page**. Clicking on the **Network > Zones** link displays the **OBJECT | Match Objects > Zones** page for applying SonicWall Gateway Anti-Virus on zones.

## Updating SonicWall Gateway Anti-Virus Signatures

By default, the SonicWall network security appliance running SonicWall Gateway Anti-Virus automatically checks the SonicWall signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your SonicWall Gateway Anti-Virus database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWall Gateway Anti-Virus signature updates are secured. The SonicWall network security appliance must first authenticate itself with a pre-shared secret, created during the SonicWall Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

## Enabling SonicWall Gateway Anti-Virus

You must select the **Enable Gateway Anti-Virus** checkbox in the **Gateway Anti-Virus Global Settings** section to enable SonicWall Gateway Anti-Virus on your SonicWall network security appliance.

You must specify the zones you want SonicWall Gateway Anti-Virus protection on the **OBJECT | Match Objects > Zones** page.

## Applying SonicWall Gateway Anti-Virus Protection on Zones

You apply SonicWall Gateway Anti-Virus to zones when you add or edit a zone on the **OBJECT | Match Objects > Zones** page. From the **Security Services > Gateway Anti-Virus** page, you can quickly display the **OBJECT | Match Objects > Zones** page by clicking the link in the **Note: Enable the Gateway Anti-Virus per zone** from the **OBJECT | Match Objects > Zones** page. in the **SonicWall Gateway Anti-Virus Status** section.

## Specifying Protocol Filtering

Application-level awareness of the type of protocol that is transporting the violation allows SonicWall Gateway Anti-Virus to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

### Topics:

- [Enabling Inbound Inspection](#)
- [Enabling Outbound Inspection](#)
- [Restricting File Transfers](#)
- [Resetting Gateway Anti-Virus Settings](#)

## Enabling Inbound Inspection

By default, SonicWall Gateway Anti-Virus inspects all inbound HTTP, FTP, IMAP, SMTP and POP3 traffic. Generic TCP Stream can optionally be enabled to inspect all other TCP-based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

Within the context of SonicWall Gateway Anti-Virus, the **Enable Inbound Inspection** protocol traffic handling refers to:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone.
- Non-SMTP traffic from a Public zone destined to an Untrusted zone.
- SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.

### SMTP TRAFFIC

	To	Trusted	Encrypted	Wireless	Public	Untrusted
<b>From</b>						
Trusted		✓	✓	✓		
Encrypted		✓	✓	✓		
Wireless		✓	✓	✓		
Public		✓	✓	✓	✓	✓
Untrusted		✓	✓	✓	✓	✓

### ALL OF THE OTHER TRAFFIC

	To	Trusted	Encrypted	Wireless	Public	Untrusted
<b>From</b>						
Trusted		✓	✓	✓	✓	✓
Encrypted		✓	✓	✓	✓	✓
Wireless		✓	✓	✓	✓	✓
Public						✓
Untrusted						

## Enabling Outbound Inspection

The **Enable Outbound Inspection** feature is available for HTTP, FTP, SMTP, and TCP traffic

# Restricting File Transfers

For each protocol, except TCP Stream, you can restrict the transfer of files with specific attributes by clicking on the Settings button under the protocol in the **Gateway Anti-Virus Global Settings** section.

## Topics:

- [FTP Settings](#)
- [Exclusion Settings](#)

## FTP Settings

These restrict-transfer FTP Settings include:

- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (for example, HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files.

Packers are utilities that compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file.

SonicWall Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. Additional formats are dynamically added along with SonicWall Gateway Anti-Virus signature updates.

## Exclusion Settings

Address objects selected from the restrict-transfer FTP settings are excluded.

## Resetting Gateway Anti-Virus Settings

To reset all Gateway Anti-Virus settings to factory default values

1. Click the **Reset Gateway AV Settings** button. A confirmation message displays.
2. Click **OK**.

## Configuring Gateway Anti-Virus Settings

Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Config View** dialog, which allows you to configure clientless notification alerts and create a SonicWall Gateway Anti-Virus exclusion list.

## Topics:

- [Configuring Gateway Anti-Virus Settings](#)
- [Configuring HTTP Clientless Notification](#)
- [Configuring a SonicWall GAV Exclusion List](#)

# Configuring Gateway Anti-Virus Settings

## *To configure Gateway Anti-Virus options:*

1. To suppress the sending of e-mail messages (SMTP) to clients from SonicWall Gateway Anti-Virus when a virus is detected in an e-mail or attachment, select **Disable SMTP Responses**. This option is not selected by default.
2. The EICAR Standard Anti-Virus Test file is a special virus simulator file that checks and confirms the correct operation of the SonicWall Gateway Anti-Virus service. To suppresses the detection of the EICAR, select **Disable detection of EICAR test virus**. This option is selected by default.
3. To allow the sending of byte serving, the process of sending only a portion of an HTTP message or file, select **Enable HTTP Byte-Range requests with Gateway AV**. This option is selected by default.  

The SonicWall Gateway Anti-Virus security service, by default, suppresses the use of HTTP Byte-Range requests to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.
4. To allow the use of the FTP REST request to retrieve and reassemble sectional messages and files, select **Enable FTP 'REST' requests with Gateway AV**. This option is selected by default.
5. The Gateway Anti-Virus service, by default, suppresses the use of the FTP 'REST' (restart) request to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.
6. To suppresses the scanning of files, or parts of files, that have high compression rates, select **Do not scan parts of files with high compression rates**. This option is selected by default.
7. To block files containing multiple levels of zip and/or gzip compression, select **Block files with multiple levels of zip/gzip compression**. This option is selected by default.
8. To have the Gateway Anti-Virus service in detection-only mode, which only detects and logs virus traffic without stopping such traffic, select **Enable detection-only mode**. This option is not selected by default.

## Configuring HTTP Clientless Notification

The HTTP Clientless Notification feature notifies users when Gateway Anti-Virus detects an incoming threat from an HTTP server.

If this feature is disabled, when GAV detects an incoming threat from an HTTP server, Gateway Anti-Virus blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that Gateway Anti-Virus detected a threat from the HTTP server.

① | **TIP:** The HTTP Clientless Notification feature is also available for SonicWall Anti-Spyware.

### To configure this feature:

1. Select **Enable HTTP Clientless Notification Alerts**. This option is selected by default.
2. Optionally, enter a message in the **Message to Display when Blocking** field. The default message is `This request is blocked by the Firewall Gateway Anti-Virus Service.`

① **TIP:** You can configure a timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Settings** heading.

## Configuring a SonicWall GAV Exclusion List

Any IP addresses listed in the exclusion list bypass virus scanning on their traffic. The **Gateway AV Exclusion List** section provides the ability to either select an Address Object or define a range of IP addresses whose traffic will be excluded from SonicWall Gateway Anti-Virus scanning.

⚠ **CAUTION:** Use caution when specifying exclusions to SonicWall Gateway Anti-Virus protection.

### To add an IP address range for exclusion:

1. Navigate to **POLICY | Security Services > Gateway Anti-Virus**.
2. Scroll to the **Gateway Anti-Virus Global Settings** section.
3. Click the **Configure Gateway AV Settings** button.
4. Select **Enable Gateway AV Exclusion List** in the **Gateway AV Exclusion List** section to enable the exclusion list.
5. Select one of these:
  - Use **Address Object** radio button
    1. Select an address object from the **Use Address Object** list.
    2. Click **OK**.
  - Use **Address Range** radio button.
    1. Click the **Add** icon. The **Add GAV Range Entry** dialog displays.
    2. Enter the IP address range in the **IP Address From** and **IP Address To** fields.
    3. Click **OK**. Your IP address range appears in the **Gateway AV Exclusion List** table.
      1. To change an entry, click the **Edit** icon in the **Configure** column
      2. To delete an entry, click the **Delete** icon.
      3. To delete all entries in the exclusion list, click the **Delete All** button.
  - 4. Click **OK**.

## Configuring Cloud Gateway Anti-Virus

### To enable the Cloud Gateway Anti-Virus feature:

1. Navigate to **Security Services > Gateway Anti-Virus > Cloud Anti-Virus Global Settings**.
2. Select **Enable Cloud Anti-Virus Database**. (This option is selected by default.)

Optionally, certain cloud-signatures can be excluded from being enforced to alleviate false positive problems or to enable downloading specific virus files as necessary.

### To configure the exclusion list:

1. Click **Cloud AV DB Exclusion Settings**. The **Add Cloud AV Exclusion** dialog displays.
2. In the **Cloud AV Signature ID** field, enter the signature ID. The ID must be a numeric value.
3. Click **Add**.  
Repeat the previous two steps for each signature ID you want to add.
4. Optionally, to update a signature ID:
  - a. Select the signature ID in the **List** field.
  - b. Enter the updated signature in the **Cloud AV Signature ID** field.
  - c. Click **Update**.
5. Optionally, to delete:
  - A signature ID, select the ID in the **List** field, and then click **Remove**.
  - All signatures, click **Remove All**.
6. Optionally, to view the latest information on a signature, select the signature ID in the list and click the **Sig Info** button. The information for the signature is displayed on the SonicAlert website.
7. When you have finished configuring the Cloud AV exclusion list, click **OK**.

## Viewing SonicWall Gateway Anti-Virus Signatures

The Gateway Anti-Virus Signatures section allows you to view the contents of the SonicWall Gateway Anti-Virus signature database. All the entries displayed in the Gateway Anti-Virus Signatures table are from the SonicWall Gateway Anti-Virus signature database downloaded to your SonicWall network security appliance. The number of malware family signatures is displayed above the table.

① | **NOTE:** Signature entries in the database change over time in response to new threats.

### Topics:

- [Displaying Signatures](#)
- [Navigating the Gateway Anti-Virus Signatures Table](#)
- [Searching the Gateway Anti-Virus Signature Database](#)

## Displaying Signatures

You can display the signatures in a variety of views:

① | **TIP:** When you filter the signature, the number of signatures found is displayed along with the total number of signatures in the database.

- **View Style** – Select one of these from the First Letter drop-down menu:
  - **All Signatures** - Displays all the signatures in the table, 50 to a page.
  - **0 – 9** - Displays signature names beginning with the number you select from the menu.
  - **A – Z** - Displays signature names beginning with the letter you select from menu.

- **Search String** - Displays signatures containing a specific string:
  1. Enter the string in the **Lookup Signatures Containing String** field.
  2. Click the **Magnifying Glass** icon.

## Navigating the Gateway Anti-Virus Signatures Table

The SonicWall Gateway Anti-Virus signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. For information about navigating through the table, see *About SonicOS*.

## Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the **Search** icon.

Only the signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.



# Anti-Spyware Service

SonicWall Anti-Spyware is included in the SonicWall Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS) unified threat management solution. Together, SonicWall Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service deliver a comprehensive, real-time, gateway security solution for your entire network.

After activating your SonicWall Anti-Spyware license, you must enable and configure SonicWall Anti-Spyware on the management interface. Only when this is done can the anti-spyware policies be applied to your network traffic.

For instructions on setting up SonicWall Anti-Spyware Service, refer to the *SonicWall Anti-Spyware Service Administration Guide* available on the SonicWall website at: <https://www.sonicwall.com/support/technical-documentation>.

To enable and configure Anti-Spyware for your SonicWall network security appliance, navigate to **POLICY | Security Services > Anti-Spyware**. The Anti-Spyware management interface screen is divided into these sections:

- [Anti-Spyware Status](#)
- [Anti-Spyware Global Settings](#)
- [Signature Groups](#)
- [Protocols](#)
- [Anti-Spyware Signatures](#)

## Anti-Spyware Status

This section of the screen displays status information on the signature database, your SonicWall Anti-Spyware license, and other details. It gives the date and time of the latest available database. If you want to enable Anti-Spyware Service for a zone, click on the word **Zone** for a link to the **Zone** screen.

# Anti-Spyware Global Settings

- **Enable Anti-Spyware** - Select this option to make key settings available for enabling Anti-Spyware on your SonicWall network security appliance.
- **WAN, LAN/WorkPort, and DMZ/HomePort/WLAN/OPT** - After you enable Anti-Spyware, these three interface checkboxes become available. Check the ones where you want to activate the spyware. SonicWall Anti-Spyware must first be globally enabled on your SonicWall network security appliance.

## Signature Groups

- You can select different protection for each of three different danger levels:
  - **High Danger Level Spyware**
  - **Medium Danger Level Spyware**
  - **Low Danger Level Spyware**
- **Prevent All** - Select this option to detect, log, and prevent all attacks of this level.
  - △ **CAUTION:** SonicWall recommends enabling **Prevent All** for **High Danger Level Spyware** and **Medium Danger Level Spyware** signature groups to provide anti-spyware protection against the most damaging and disruptive spyware applications. You can also enable **Detect All** for spyware logging and alerting.
- **Detect All** - Select this option to detect and log only.
- **Log Redundancy Filter (Seconds)** - To prevent the log from becoming overloaded with entries for the same attack, enter a value in the field. For example, if you entered a value of 30 seconds and there were 100 SubSeven attacks during that period of time, only one attack would be logged during that 30 second period.
- **Configure Settings** - This is one of the buttons below the attack level chart. It displays the **Anti-Spyware Settings** dialog box.
  - **Anti-Spyware Settings**
    - **Disable SMTP Responses** - Click this checkbox to suppress the sending of email messages (SMTP) to clients from SonicWall Anti-Spyware when a virus is detected in an email or attachment.
  - **HTTP Clientless Notification**
    - **Enable HTTP Clientless Notification Alerts** - Checking this box allows the message in the box below to be shown when blocking a request.
  - **Anti-spyware Exclusion List**
    - **Enable Anti-Spyware Exclusion List** - Click this checkbox to allow the spyware to be limited by an exclusion list. The security appliance bypasses Anti-Spyware enforcement for a specified address object or IP range. Selecting this box makes the next fields available to identify the addresses of the excluded objects.
    - Select an address object or an address range to add to the exclusion list.

- **Update Signature Database** - Click to refresh the list on the lower part of this page. A dialog box appears requesting more information about the schedule for your changes.
- **Reset Settings** - Click to reset the settings to the factory defaults. A dialog box appears requesting more information about the schedule for your changes.

## Protocols

You can choose on which protocols you want to **Enable Inbound Inspection** by the Anti-Spyware software.

- Click the checkbox for each selected protocol.
- Enable **Inspection of Outbound Spyware Communication** - Clicking this choice makes the outbound traffic available for inspection.

## Anti-Spyware Signatures

SonicWall Anti-Spyware allows you to configure anti-spyware policies at the category and signature level, to provide flexible granularity for tailoring SonicWall Anti-Spyware protection based on your network environment requirements. You can apply these custom SonicWall Anti-Spyware policies to Address Objects, Address Groups, and User Groups, as well as create enforcement schedules.

When you click **Config** on the **Signature** row, you can configure these fields in the **Anti-Spyware Signature Settings** dialog box:

Field	Description
<b>Product Name</b>	The name in the row you chose to configure
<b>Prevention</b>	Allows you to enable and disable anti-spyware prevention for the device
<b>Detection</b>	Allows you to enable and disable anti-spyware detection for the device
<b>Included Users/Groups</b>	Applies the anti-spyware settings to members of the following group types: All, Administrators, Everyone, Guest Services, Trusted Users, Content Filtering Bypass, and Limited Administrators
<b>Excluded Users/Groups</b>	Does not apply the anti-spyware settings to members of the following group types: All, Administrators, Everyone, Guest Services, Trusted Users, Content Filtering Bypass, and Limited Administrators
<b>Included IP Address Range</b>	Allows you to apply the anti-spyware settings to all users that fall within a specified IP address range of a specified category
<b>Excluded IP Address Range</b>	Allows you to exclude all users that fall within a specified IP address range of a specified category
<b>Schedule</b>	Allows you to set a schedule
<b>Log Redundancy Filter</b>	Check this box to set the filter
<b>Use Product Settings in seconds</b>	If the filter box is checked, this setting is not available

# Intrusion Prevention Service

The Intrusion Prevention Service (IPS) is a subscription-based service that is frequently updated to protect your networks from new attacks and undesired uses that expose your network to potential risks.

## Topics:

- [About Intrusion Prevention Service](#)
- [Enabling Intrusion Prevention Services](#)
- [IPS Status](#)
- [IPS Global Settings](#)
- [Intrusion Prevention Service Policies](#)

## About Intrusion Prevention Service

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection (DPI) engine for extended protection of key network services such as Web, email, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities, as well as worms, Trojans, and peer-to-peer, spyware and back door exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly-discovered application and protocol vulnerabilities. SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

Deep Packet Inspection (DPI) looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds anomalies in the traffic and reacts, preventing the traffic from passing through.

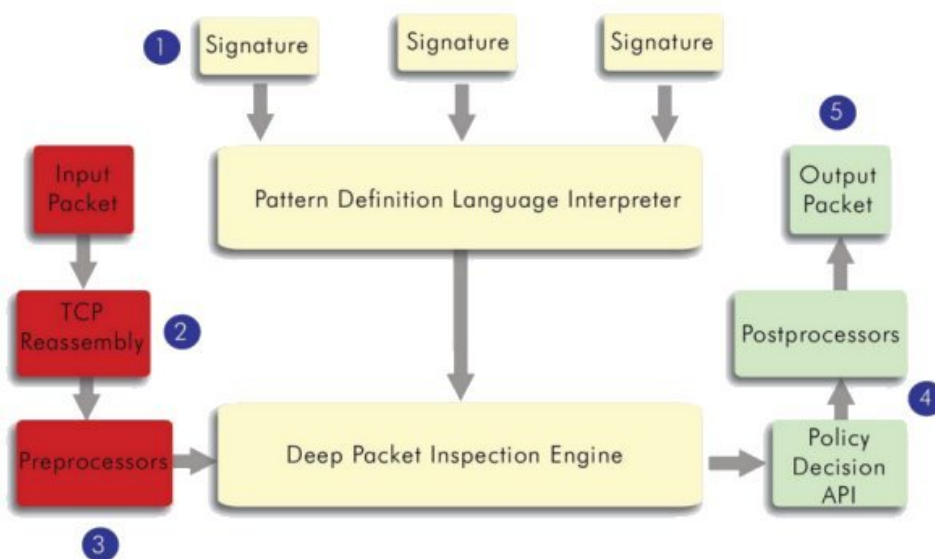
Deep Packet Inspection is a technology that allows a SonicWall security appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet, as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWall network security appliance, as well as prevent them (such as dropping the packet or resetting the TCP connection). SonicWall's DPI technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation had occurred.

Deep Packet Inspection (DPI) technology enables your SonicWall network firewall appliance to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWall Intrusion Prevention Service. SonicWall's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWall Distributed Enforcement Architecture.

SonicWall Deep Packet Inspection Architecture works like this:

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request might be URL encoded and so the request is URL decoded in order to execute correct pattern matching on the payload.
4. Deep Packet Inspection engine post-processors execute actions that might either simply pass the packet without modification, or could drop a packet, or could even reset a TCP connection.
5. SonicWall's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without completing any reassembly (unless the packets are out of order). This results in a more efficient use of the processor and memory for greater performance.

## SonicWALL DEEP PACKET INSPECTION ARCHITECTURE



If TCP packets arrive out of order, the SonicWall IPS engine reassembles them before inspection. However, SonicWall's IPS framework supports complete signature matching across the TCP fragments without having to do a complete reassembly. SonicWall's unique reassembly-free matching solution dramatically reduces CPU and memory resource requirements.

# Enabling Intrusion Prevention Services

*To configure Intrusion Prevention settings for one or more SonicWall network security appliance:*

1. Select the global icon, a group, or a SonicWall network security appliance.
2. Navigate to **Security Services > Intrusion Prevention** and make changes as required on the three sections on the Intrusion Prevention screen.

## IPS Status

The top part of the screen gives the status of the Intrusion Prevention Service on the system. It gives the date and time of the **Latest available Signature Database**, and the zones that are IPS-enabled. If you want to enable the Intrusion Prevention Service in a certain zone, click on the word **Zone** in this section to get a link to the Zone page.

## IPS Global Settings

- **Enable IPS** - Click this setting to enable the Intrusion Prevention. After service is enabled, the next three checkboxes become available.  
Select the checkboxes of the interface ports to monitor, WAN, LAN, or DMZ/WLAN/OPT. These three checkboxes become available when **Enable IPS** is checked.
- The next section allows you to configure the level of attack to monitor and in what way. You can set different levels of protection for **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**.
  - **Prevent All** - Select this option to detect, log, and prevent all attacks of this level.
  - **Detect All** - Select this option to detect and log only.
  - **Log Redundancy Filter (Seconds)** - To prevent the log from becoming overloaded with entries for the same attack, enter a value in the field. For example, if you entered a value of 30 seconds and there were 100 SubSeven attacks during that period of time, only one attack would be logged during that 30 second period.
  - **Configure IPS Settings** - This is one of four buttons below the attack level chart. It brings up the following dialog box.
    - **IPS Exclusion List**
    - **Enable IPS Exclusion List** - Select this field to configure the SonicWall security appliance to skip Intrusion Prevention enforcement for a specified IP address object or range of address objects. The fields that follow are only available when this field is selected.
      - **Use Address Object** — Select an address object from the drop-down menu.
      - **Use Address Range** — Fill in the address range limits to exclude. If the address range is selected, you can Add or Delete All of the choices.

- **Update IPS Signature Database** - Select to force the firmware to download all signatures.
- **Reset IPS Settings & Policies** - Click to reset your IPS settings to the defaults.
- **Import CSV File** - This button imports the CSV file.
- Click **OK** or **Cancel** when you are done with this page.

**Save** - brings up a dialog box requesting more information about the schedule and persistence of the individual changes you have made.

**Cancel** - clears all the settings on the screen.

## Intrusion Prevention Service Policies

This section allows the administrator to configure settings for individual attacks.

1. Locate the type of attack that you would like to view. To sort by category, select a category from the **Categories** list. To sort by priority, select a priority level from the **Priority** list.
2. After locating a type of attack to configure, click **Config/Edit** on its row. A dialog box appears where you can give specific information about the **IPS Signature Settings** for the selected attack. The top part of the dialog box is populated with the information from the selected **Signature** row.
3. Configure the fields in the dialog box for each type of attack you need to edit:
  - **Prevention** - Select whether attack prevention for this type of attack is enabled, disabled, or uses the default global settings for the attack category from the list.
  - **Detection** - Select whether attack detection for this type of attack is enabled, disabled, or uses the default global settings for the attack category from the list.
  - **Included Users/Groups** - Select which users or groups to include for this attack type from the list.
  - **Excluded Users/Groups** - Select which users or groups to exclude for this attack type from the list.
  - **Included IP Address Range** - Select an IP address range to include for this attack type from the list.
  - **Excluded IP Address Range** - Select an IP address range to exclude for this attack type in the list box.
  - **Schedule** - Select a time range to enforce attack protection on this attack type the list.
  - **Log Redundancy Filter (seconds)** - Enter a time span (in seconds) to set the filter or select **Use Category Settings**.
4. **Save** - This selection returns you to the Intrusion Prevention page. Your changes have been applied.
5. **Cancel** - This selection discards your changes.

# Configuring Geo-IP Filters

The **Geo-IP Filter** feature allows you to block connections to or from a geographic location. The SonicWall network security appliance uses the IP address to determine to the location of the connection. The **Geo-IP Filter** feature also allows you to create custom country lists that affect the identification of an IP address.

The **Geo-IP Filter** feature also allows you to create a custom message when you block a web site.

You can also use the **Geo-IP Filter > Diagnostics** tool to show resolved locations, monitor Geo-IP cache statistics, custom countries statistics, and look up GEO-IP servers.

## Topics:

- [Configuring Geo-IP Filtering](#)
- [Creating Custom Country Lists](#)
- [Customizing Web Block Page Settings](#)
- [Using Geo-IP Filter Diagnostics](#)

## Configuring Geo-IP Filtering

The **Settings** page gives a group of settings that can be configured for Geo-IP Filtering. Several of the settings have (information) icons next to them that give screen tips about that setting.

- **Block connections to/from countries selected in the Countries tab** - This option is selected by default. If this option is enabled, all connections to/from the selected list of countries are blocked. You can specify an exclusion list to exclude blocking for selected IPs. When this option is selected, the next two options become available.
  - **All Connections** - This selects one of the two modes of Geo-Filter. All connections to and from the firewall are filtered. This option is selected by default.
  - **Firewall Rule-Based Connections** - With this selection only connections that match an access rule configured on the firewall are filtered for blocking.
- **Block all connections to public IPs if GeoIP DB is not downloaded** - This option is not selected by default. If the Geo-IP database is not downloaded, this selection drops all attempted connections from public IP addresses.
- **Enable Custom List** - This option is not selected by default. Custom lists are sometimes used to correct a false country assignment for an IP address. If the checkbox is selected, the Override Firewall Countries by Custom List is made available.



- **Override Firewall Countries by Custom List** - This selection is only available if Enable Custom List is clicked. It allows your custom list to override the firewall list where there are differences. Unless you select this Override, the firewall list takes precedence, even when you have enabled a custom list.
- **Enable Logging** - This option is not selected by default. It enables logging of filter events.

The **Countries** page gives a group of settings that can be configured for Geo-IP Filtering to block specific countries.

- **Blocked Country table** - Click the checkbox for the countries to be blocked. By default, no countries are blocked. By clicking on the checkbox at the top of the table, you can select all countries, then exclude countries from blocking by clicking on them separately.
- **Block All Unknown countries** - Select this option to block any countries that are not listed. All connections to unknown public IPs are blocked. This option is not selected by default.
- **Geo-IP Exclusion Object** - This setting allows you to configure an exclusion list of all connections to approved IP addresses.

Select an address group from the list. The default is **Default Geo-IP and Botnet Exclusion Group**.

The **Geo-IP Exclusion Object** is a network address object group that specifies a group or a range of IP addresses to be excluded from the Geo-IP filter blocking. All IP addresses in the address object or group are allowed, even if they are from a blocked country.

For example, if all IP addresses coming from Country A are set to be blocked and an IP address from Country A is detected, but it is in the Geo-IP Exclusion Object list, then traffic to and from this IP address is allowed to pass.

For this feature to work correctly, the country database must be downloaded to the firewall. The **Status** indicator at the top right of the page turns yellow if this download fails. Green status indicates that the database has been successfully downloaded.

For the country database to be downloaded, the firewall must be able to resolve the address `geodnsd.global.SonicWall.com`.

When a user attempts to access a web page that is from a blocked country, a block page message is displayed on the user's web browser.

If a connection to a blocked country is short-lived and the firewall does not have a cache for the IP address, then the connection might not be blocked immediately. As a result, connections to blocked countries might occasionally appear in the App Flow Monitor. However, additional connections to the same IP address are blocked immediately.

Click:

- **Accept** to confirm your changes.
- **Reset** to cancel your changes.

# Creating Custom Country Lists

This section allows you to create a custom list of IP addresses to either block or allow. This can be useful, for example, if an IP address is mistakenly associated with a blocked country, and you want it to be allowed. Having a custom country list can solve this problem by overriding the firewall country associated with the particular IP address.

For the network security appliance to use the **Custom List** first, you must enable it and select **Override Firewall List**.

## *To add a custom list address object:*

1. Click **Add** to bring up the **Add Address Location** dialog box.
2. From the **IP Address** list, select an IP Address .
3. From the **Country** list, select a country.
4. Optionally, you can add a comment in the **Comment** field.
5. Click **Save**.

## Topics:

- [Editing a Custom List Entry](#)
- [Deleting Custom List Entries](#)

# Customizing Web Block Page Settings

The Geo-IP Filter has a message that can be displayed when a user attempts to access a blocked page. You can have the message display detailed information, such as the reason why this IP address is blocked, as well as the IP address and the country from which it was detected. You can also create a custom message and include a custom logo.

- **Include Geo-IP Filter Block Details** - Select this option to show blocking details, such as reason for the blocking, the IP address, and the country. When disabled, no information is displayed. By default, this option is selected.
- **Alert text**
  - To use the default message displayed in the **Alert** text field, `This site has been blocked by the network administrator.`, click **Default Blocked Page**.
  - Fill in a custom message, if desired, to be displayed as the **Alert** text. The message can be up to 100 characters long, and can include only the following: alphanumeric, whitespace, period (.), and underscore (\_).
- **Base64-encoded Logo Icon** - In this field, you can specify a Base 64-encoded GIF icon to be displayed instead of the default SonicWall logo.
  - ① **NOTE:** Make sure this icon is valid and make the size as small as possible. The recommended size is 400 x 65 pixels.

- **Preview** - Click to display the Web Site Page preview window. This gives you a chance to verify your configuration and make changes if needed.
- **Default Blocked Page** - Reset the blocked message back to the default content.

**To set the web block page settings back to default:**

1. Click **Default Blocked Page**.  
① | **IMPORTANT:** The **Base64-encoded Logo Icon** field must be left blank.
2. Click **Accept**.
3. Click **Update**. A dialog box displays that requests information about the schedule for your updates, and editing the fields selected for the Change creation.

## Using Geo-IP Filter Diagnostics

The **Security Services > GEO-IP Filter > Diagnostics** page provides access to several tools:

- [Geo-IP Cache Statistics](#)
- [Custom Countries Statistics](#)
- [Show Resolved Locations](#)
- [Incorrectly Marked Address](#)
- [Check GEO Location Server Lookup](#)

## Geo-IP Cache Statistics

The **Geo-IP Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**
- **Current Entry Count**
- **Max. Entry Count**
- **Location Map Count**

## Custom Countries Statistics

The **Custom Countries Statistics** table contains this information about the number of entries in the list and the number of times lookups have occurred for the entries:

- **No of Entries**
- **No of Times Called**
- **No of Times Not Looked-up**
- **No of Times Resolved**

## Show Resolved Locations

When you click the **Show Resolved Locations** button, a pop-up table of resolved IP addresses displays this information:

- **Index**
- **IP Address**
- **Country**

## Check GEO Location Server Lookup

The Geo-IP Filter also provides the ability to look up IP addresses to determine:

- Domain name or IP address
- The country of origin and whether it is classified as a Botnet server

① **NOTE:** The similar Botnet Location Server Lookup tool can also be accessed from the **Security Services > Botnet Filter** page.

*To look up a GEO server:*

1. Navigate to **POLICY | Security Services > GEO-IP Filter**.
2. Click **Diagnostics**.
3. Scroll to the **Check GEO Location Server Lookup** section.
4. In the Lookup IP field, enter the IP address .
5. Click **Go**.

Details on the IP address display below the Result heading.

## Incorrectly Marked Address

If you think an address is marked as part of a country incorrectly, you can report the issue by clicking on the **Geo-IP Status Lookup** link in the **Note** on the **POLICY | Security Services > GEO-IP Filter** page.

The link displays the **Submit IP for Geolocation Review** page.

# Configuring Botnet Filters

The **Botnet Filter** feature allows you to block connections to or from Botnet command and control servers, and make custom Botnet lists. It also allows you to create a custom message to send when you block a web site, or to allow dynamic Botnet HTTP authentication. Many of the selections on this page have an **Information** icon that you can hover over for a screen tip.

## Topics:

- [Configuring Botnet Filtering](#)
- [Creating Custom Botnet Lists](#)
- [Configuring Dynamic HTTP Authentication](#)
- [Customizing Web Block Page Settings](#)
- [Using Botnet Filter Diagnostics](#)
- [Displaying the Status of the Botnet Feature and Database](#)

## Configuring Botnet Filtering

### *To configure Botnet filtering:*

1. Navigate to **POLICY | Security Services > Botnet Filter**.
2. Click **Settings**.
3. To block all servers that are designated as Botnet command and control servers, select the **Block connections to/from Botnet Command and Control Servers** option. All connection attempts to/from Botnet command and control servers will be blocked. This option is not selected by default. If this option is selected, the radio buttons and the **Block all connections to public IPs if BOTNET DB is not downloaded** option become available. To exclude selected IPs from this blocking behavior, use exclusion lists as described in the following steps and/or create a custom Botnet list as described in [Creating Custom Botnet Lists](#).
4. If **Block connections to/from Botnet Command and Control Servers** is selected, these options become available:
  - a. Select one of the following two modes for Botnet Filtering:
    - **All Connections:** All connections to and from the firewall are filtered. This is the default Botnet block mode.
    - **Firewall Rule-Based Connections:** Only connections that match an access rule configured on the firewall are filtered.

- b. If you want to block all connections to public IPs when the Botnet database is not downloaded, select the **Block all connections to public IPs if BOTNET DB is not downloaded**. This option is not selected by default.
5. To enable the **Custom Botnet List**, select **Enable Custom Botnet List**. This option is not selected by default.
 

If **Enable Custom Botnet List** is not selected, then only the Botnet database that resides on the network security appliance is searched. **Go to Step 6.**

Enabling a custom list by selecting **Enable Custom Botnet List** can affect country identification for an IP address:

  - a. During Botnet identification, the custom Botnet list is searched first.
  - b. If the IP address is not resolved, the firewall's Botnet database is searched.

If an IP address is resolved from the custom Botnet list, it can be identified as either a Botnet IP address or a non-Botnet IP address, and action taken accordingly.
6. Select **Enable logging** to log Botnet Filter-related events.
7. Optionally, you can configure an exclusion list of all IPs belonging to the configured address object/address group. All IPs belonging to the list are excluded from being blocked. To enable an exclusion list, select an address object or address group from the **Botnet Exclusion Object** list.
 

The default exclusion object is **Default Geo-IP and Botnet Exclusion Group**. You can create your own address object or address group object.
8. Click **Accept**.

## Creating Custom Botnet Lists

<b>Address Object</b>	Name of the address object or address group object.
<b>Botnet</b>	Icon indicating whether the entry was defined as a Botnet when created. A black circle indicates a Botnet, a white circle a non-Botnet.
<b>Comments</b>	Any comments you added about the entry.
<b>Configure</b>	Contains Edit and Delete icons for the entry.
<b>Total</b>	Displays the number of entries in the <b>Custom Botnet List</b> .

An IP address can be wrongly marked as Botnet. This kind of misclassification can cause incorrect/unwanted filtering of an IP address. Having a custom Botnet list can solve this problem by overriding the Botnet tag for a particular IP address.

### Topics:

- [Creating a Custom Botnet List](#)
- [Editing Custom Botnet List Entries](#)
- [Deleting Custom Botnet List Entries](#)

# Creating a Custom Botnet List

① **IMPORTANT:** For the firewall to use the custom Botnet list, you must enable it as described in [Configuring Botnet Filters](#).

## To create a custom Botnet list:

1. Navigate to the **POLICY | Security Services > Botnet Filter**.
2. Click **Settings**.
3. Click **Custom Botnet List**.
4. Click the **Add** icon. The **Add Custom Botnet List** dialog displays.
5. Select an IP address object or create a new address object from the **A Botnet IP Address** list:
  - ① **IMPORTANT:** An address object cannot overlap any other address objects in the custom country list. Different address objects, however, can have the same country ID.
    - **Create new address object...** – the **Add Address Object** dialog displays.
      1. You create a new address object as described in *SonicWall SonicOS 7 Policies*, with restrictions. Allowed types are:
        1. **Host**
        2. **Range**
        3. **Network**
        4. A group of any combination of the first three typesAll other types are disallowed types and cannot be added to the custom Botnet list.
    - **Create new address group...** – the **Add Address Object Group** dialog displays.

You create a new address object as described in *SonicWall SonicOS 7 Policies*
    - Already defined address object or address group
6. If this address object is a known Botnet, select the **Botnet** checkbox.
7. Optionally, add a comment in the Comment field.
8. Click **OK**.

# Editing Custom Botnet List Entries

## To edit a custom Botnet list entry:

1. In the **Custom Botnet List** table, click the **Edit** icon in the **Configure** column for the entry to be edited. The **Add Custom Botnet List** dialog displays the entry.
2. Make your changes.
3. Click **OK**.

The Custom Botnet List table is updated.

# Editing Custom Botnet List Entries

## *To edit a custom Botnet list entry:*

1. In the **Custom Botnet List** table, click the **Edit** icon in the **Configure** column for the entry to be edited. The **Add Custom Botnet List** dialog displays the entry.
2. Make your changes.
3. Click **OK**.

The Custom Botnet List table is updated.

# Configuring Dynamic HTTP Authentication

With SonicOS, username and passwords for HTTP URLs in the dynamic Botnet configuration are accepted, and the information is transmitted in the HTTP header so the network security appliance has the required information.

## *To configure dynamic HTTP authentication:*

1. Navigate to **POLICY | Security Services > Botnet Filter**.
2. Click **Dynamic Botnet List Server**.
3. Select **Enable botnet list download periodically**. This option is not selected by default.
4. From **Download Interval**, select the frequency of downloads:
  - **5 minutes** (default)
  - **15 minutes**
  - **1 hour**
  - **24 hours**

The network security appliance downloads the Botnet file from the server at the specified interval.

5. From **Protocol**, select the protocol in which the network security appliance has to communicate with the backend server to retrieve the file:
  - **FTP** (default)
  - **HTTPS**
6. In the **Server IP Address** field, enter the IP address of the server to which the Botnet list file will be downloaded.
7. In the **Login ID** field, enter the login ID the network security appliance is to use to connect to the server.
8. In the **Password** field, enter the password the network security appliance is to use to connect to the server.
9. In the **Directory Path** field, enter the directory path the firewall from which the network security appliance retrieves the Botnet file. This server directory path is relative to the default root directory.
10. In the **File Name** field, enter the name of the file on the server to be downloaded .
11. Click **Accept**.



# Customizing Web Block Page Settings

The **Botnet Filter** has a default message that is displayed when a page is blocked. You can customize this message and include your own logo.

**To create a custom message and include a custom logo:**

1. Navigate to **POLICY | Security Services > Botnet Filter**.
2. Ensure the **Include Botnet Filter Block Details** option is selected. This option is selected by default.  
When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, this option hides all information.
3. Do one of the following:
  - To use the default message displayed in the **Alert** text field, This site has been blocked by the network administrator., click the **Default Blocked Page** button.
  - Specify a custom message to be displayed in the **Botnet Filter Block** page in the **Alert** text field. Your message can be up to 100 characters long.
4. Optionally, in the **Base64-encoded Logo Icon** field, you can specify a Base 64-encoded GIF icon to be displayed as well.  
**NOTE:** Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65 pixels.
5. To see a preview of your customized message and logo (or the default message and logo), click the **Preview** button. A warning message displays.
6. Click **OK**. The **Web Site Blocked** message displays.
7. Close the **Web Site Blocked** message.
8. Click **Accept**.

## Using Botnet Filter Diagnostics

The **POLICY | Security Services > Botnet Filter** page provides access to several tools:

- [Botnet Cache Statistics](#)
- [Botnets Statistics](#)
- [Show Resolved Botnet Locations](#)
- [Check Botnet Server Lookup](#)
- [Incorrectly Marked Address](#)

## Botnet Cache Statistics

The **Botnet Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**
- **Current Entry Count**
- **Max. Entry Count**
- **Botnets Detected**

## Botnets Statistics

The **Diagnostics** view displays statistics for both custom and dynamic Botnets. Both the **Custom Botnets Statistics** and **Dynamic Botnet Statistics** tables display the same information about the number of entries in the list and the number of times lookups have occurred for the entries:

- **No of Entries**
- **No of Times Called**
- **No of Times Not Looked-up**
- **No of Times Resolved**

## Show Resolved Botnet Locations

When you click on **Show Botnets** in the **Diagnostics** section, a table of resolved IP addresses displays with this information:

- **Index**
- **IP Address** – IP address of the Botnet

## Check Botnet Server Lookup

The **Botnet Filter** also provides the ability to look up IP addresses to determine:

- Domain name or IP address
- Country of origin and whether the server is classified as a Botnet server

The Botnet Server Lookup tool can also be accessed from the System > Diagnostics page.

### ***To look up a Botnet server:***

1. Navigate to **POLICY | Security Services > Botnet Filter**.
2. Click **Diagnostics**.
3. Scroll to the **Check BOTNET Server Lookup** section.
4. In the **Lookup IP** field, enter the IP address.
5. Click **Go**.

Details on the IP address are displayed below the Result heading.

## Incorrectly Marked Address

If you believe that a certain address is marked as a Botnet incorrectly, or if you believe an address should be marked as a Botnet, report this issue at SonicWall Botnet IP Status Lookup by either:

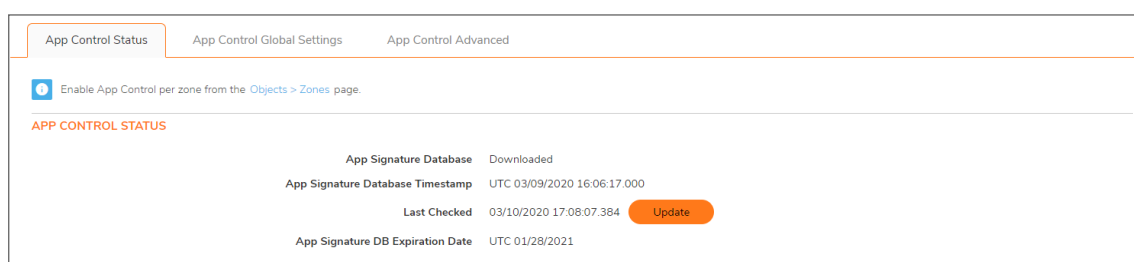
- Clicking on the link in the **Note** in the **POLICY > Security Services > Botnet Filter** page
- Going to [SonicWall Botnet IP Status Lookup](#).

## Displaying the Status of the Botnet Feature and Database

- To display the status of the Botnet feature and database, click the **Status** icon. A popup with the status displays.
- To close the popup, click the **X**.

# Configuring App Control

App Control is a licensed service and you must enable it to activate the functionality.



The **POLICY | Security Services > App Control** page provides a way to configure global App Control policies using categories, applications, and signatures. You can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. When enabled, the category, application, or signature is blocked or logged globally without the need to create a policy on the **POLICY | Rules and Policies > App Rules** page. All application detection and prevention configuration is available on the **POLICY | Rules and Policies > App Control** page.

① **NOTE:** When **Enable App Control** is selected from the **POLICY | Security Services > App Control | App Control Global Settings** page, the **dpi=1** Syslog tag is seen in the **Connection Closed Syslog** messages for all traffic that passed through Deep Packet Inspection. Traffic that did not pass through DPI shows **dpi=0** in the **Connection Closed Syslog** messages. For more information about the Index of Syslog Tags Field Descriptions or Syslog examples showing the SPI tag, see the *SonicOS Log Events Administration Guide*.

**You can configure the following settings on this page:**

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these App Control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here, and use those match objects in an App Rules policy. See *About Application List Objects* and *Configuring Application List Objects* for more information.

① **VIDEO:** Informational videos with App Control configuration examples are available online at: <https://www.sonicwall.com/support/video-tutorials>.

## Topics:

- [About App Control Policy Creation](#)
- [Viewing App Control Status](#)
- [About App Control Global Settings](#)
- [Configuring App Control Global Settings](#)
- [Viewing Signatures](#)
- [Configuring App Control by Category](#)
- [Configuring App Control by Application](#)
- [Configuring App Control by Signature](#)

# About App Control Policy Creation

The configuration method on the **POLICY | Rules and Policies > App Control** page allows granular control of specific categories, applications, or signatures. This includes granular logging control, granular inclusion and exclusion of users, groups, or IP address ranges, and schedule configuration. The settings here are global policies and independent from any custom App Rules policy.

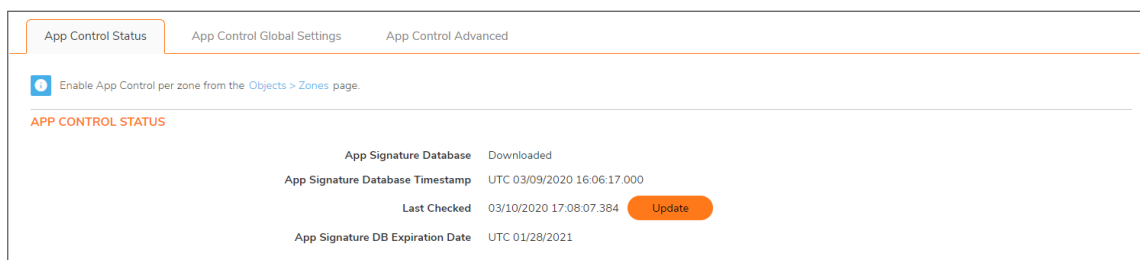
### *You can configure the following settings on this page:*

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these App Control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here or on the **OBJECT | Match Objects > Addresses** page, and use those match objects in an App Rules policy. This allows you to use the wide array of actions and other configuration settings available with App Rules. See *About Application List Objects* for more information about this policy-based user interface for App Rules.

# Viewing App Control Status

The **App Control Status** information is displayed at the top of the **POLICY | Rules and Policies > App Control** page.



APP CONTROL STATUS	
App Signature Database	Downloaded
App Signature Database Timestamp	UTC 03/09/2020 16:06:17.000
Last Checked	03/10/2020 17:08:07.384 <a href="#">Update</a>
App Signature DB Expiration Date	UTC 01/28/2021

<b>App Signature Database</b>	Indicates whether the App Signature database has been downloaded.
<b>App Signature Database Timestamp</b>	Displays the UTC day and time the App Signature database was downloaded. To update the App Signature database, click <b>Update</b> .
<b>Last Checked</b>	Displays the day and time SonicOS last checked for updates to the App Signature database.
<b>App Signature DB Expiration Date</b>	Displays the day that the App Signature database expires.

The **App Control Status** section displays information about the signature database and allows you to update the database.

To enable App Control on a per-zone basis, click the link to the **OBJECT | Match Objects > Zones** page shown in the Note above the **App Control Status** section.

## Enabling App Control

To use App Control, it must be enabled globally and on the network zones with the application traffic.

### Enabling App Control Globally

*To enable App Control globally:*

1. Navigate to the **POLICY | Rules and Policies > App Control | App Control Global Settings** page.
2. Select **Enable App Control**.
3. Click **Submit**.

### Enabling App Control on Zones

*To enable App Control on a network zone:*

1. Navigate to the **OBJECT | Match Objects > Zones** page. Click +Add Zone or Configure to edit the desired zone. The Zone Settings dialog displays.

**Zone Settings**

General | Guest Services | Wireless | Radius Server

**GENERAL SETTINGS**

Name:

Security Type:

Allow Interface Trust:

Auto-generate Access Rules to allow traffic between zones of the same trust level:

Auto-generate Access Rules to allow traffic to zones with lower trust level:

Auto-generate Access Rules to allow traffic from zones with higher trust level:

Auto-generate Access Rules to deny traffic from zones with lower trust level:

Enable Client AV Enforcement Service:

Enable Client CF Service:

Enable DPI-SSL Enforcement Service:

Enable SSLVPN Access:

Create Group VPN:

Enable SSL Control:

Enable Gateway Anti-Virus Service:

Enable IPS:

Enable Anti-Spyware Service:

Enable App Control Service:

Enable SSL Client Inspection:

Enable SSL Server Inspection:

2. Select **Enable App Control Service**.
3. Click **Save**.

**NOTE:** App Control policies are applied to traffic within a network zone only when you select **Enable App Control Service** for that zone. App Rules policies are independent, and not affected by the App Control setting for network zones.

The **OBJECT | Match Objects > Zones** page displays a green indicator in the **App Control** column for any zones that have the App Control service enabled.

#	NAME	SECURITY T...	MEMBER INTERFACES	INTERFACE TRUST	CLIENT AV	GATEWAY AV	ANTI SPYWARE	IPS	APP CONTROL	SSL CONTROL	SSL VPN ACCESS	DPI SSL CLIE
1	LAN	Trusted	X0	✓	✓	✓	✓	✓	✓			✓
2	WAN	Untrusted	X1, U0						✓			
3	DMZ	Public		✓								
4	VPN	Encrypted										
5	SSLVPN	Sslvpn										
6	MULTICAST	Untrusted										
7	WLAN	Wireless										

## Configuring Logging and Log Filter Interval

*To enable logging for all apps and specify a redundancy filter interval:*

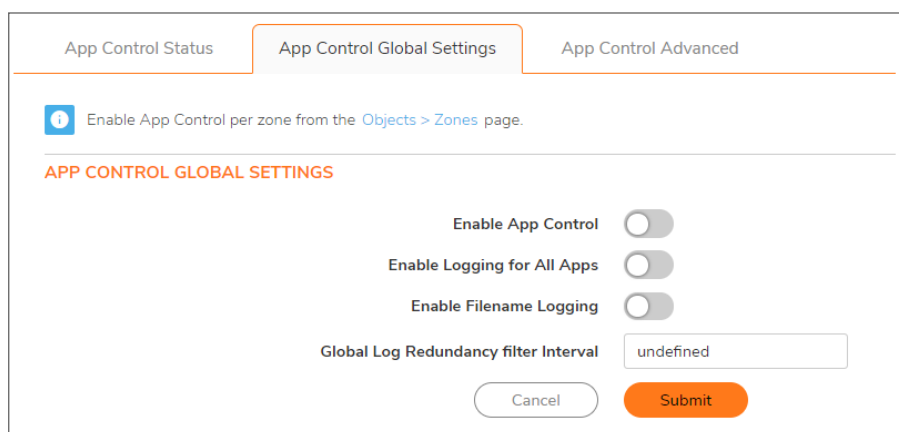
1. Navigate to the **POLICY | Rules and Policies > App Control | App Control Global Settings** page.
2. Select **Enable Logging For All Apps**.
3. Enter an interval, in seconds, for the global log redundancy filter in the **Global Log Redundancy Filter Interval** field. The range is 0 to 86400 seconds, and the default is **60** seconds.
4. Click **Submit**.

# Enabling App Control Filename Logging

To allow notification for each filename or URI of interest that has explicitly been identified as an App Control process packet or flow:

1. Navigate to the **POLICY | Rules and Policies > App Control | App Control Global Settings** page.
2. Click **Enable Filename Logging**.
3. Click **Submit**.

## Configuring App Control Global Settings



The screenshot shows the 'App Control Global Settings' page. At the top, there are three tabs: 'App Control Status', 'App Control Global Settings' (which is selected), and 'App Control Advanced'. Below the tabs, there is an information icon and a message: 'Enable App Control per zone from the [Objects > Zones](#) page.' The main section is titled 'APP CONTROL GLOBAL SETTINGS' in orange. It contains three toggle switches: 'Enable App Control', 'Enable Logging for All Apps', and 'Enable Filename Logging', all of which are currently turned off. Below these is a text input field for 'Global Log Redundancy filter Interval' with the value 'undefined'. At the bottom, there are two buttons: 'Cancel' and 'Submit'.

The **POLICY | Rules and Policies > App Control | App Control Global Settings** page contains the following global settings:

- Enable App Control
- Enable Logging For All Apps
- Enable Filename Logging
- Global Log Redundancy Filter Interval

Application Control is a licensed service and you must enable it to activate the functionality. You can also configure logging and exclusion lists for App Control and App Rules policies or reset the policies to factory defaults. For more information, see [About App Control Global Settings](#).

### Topics:

- [Enabling App Control](#)
- [Configuring Logging and Log Filter Interval](#)
- [Enabling App Control Filename Logging](#)



# About App Control Global Settings

App Control Status | **App Control Global Settings** | App Control Advanced

Enable App Control per zone from the [Objects > Zones](#) page.

**APP CONTROL GLOBAL SETTINGS**

Enable App Control

Enable Logging for All Apps

Enable Filename Logging

Global Log Redundancy filter Interval

The **POLICY | Rules and Policies > App Control** page contains the following global settings:

- **Enable App Control** – Application control is a licensed service and you must enable it to activate the functionality. It must also be enabled on a per-zone basis from the **OBJECT | Match Objects > Zones** page.
- **Enable Logging For All Apps** – If enabled, App Control and App Rules policy matches and actions are logged.
- **Enable Filename Logging** – If enabled, the administrator is notified of each filename and URIs of interest, that App Control has explicitly identified as it processes packets or flows. The notification uses the Log mechanism where the output can be shown in several message formats including:
  - SonicOS Event Logs on the **MONITOR | Logs > System Logs** page.
  - Syslog Viewer on the **DEVICE | Log > Syslog** page.

**NOTE:** For more information about Filename Logging, see the *SonicOS Log Administration Guide*.

- **Global Log Redundancy Filter Interval** – The interval, in seconds, during which multiple occurrences of the same policy match are not repetitively logged. The range is 0 to 99999 seconds, and the default is **60** seconds.

Global log redundancy settings apply to all application control events. If set to zero, a log entry is created for each policy match found in passing traffic. Other values specify the minimum number of seconds between log entries for multiple matches to the same policy. For example, a log redundancy setting of 10 will log no more than one message every 10 seconds for each policy match. Log redundancy can also be set:

- on a per-policy basis in the **Edit App Control Policy** dialog.
- on a per-category basis in the **Edit App Control Category** dialog.
- on a per-application basis in the **Edit App Control App** dialog.

Each configuration dialog has its own log redundancy filter setting that can override the global log redundancy filter setting.

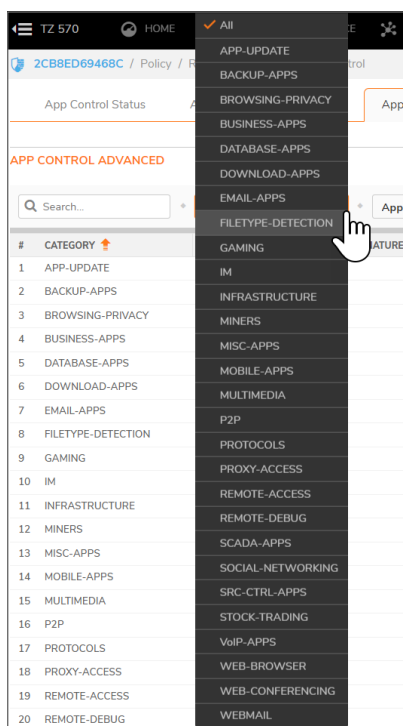
# Configuring App Control Advanced Settings

## Topics:

- [Configuring App Control Advanced by Category](#)
- [Configuring App Control Advanced by Application](#)
- [Configuring App Control Advanced by Signature](#)
- [Viewing Signatures](#)

## Configuring App Control Advanced by Category

Category-based configuration is the most broadly based method of policy configuration on the **POLICY | Rules and Policies > App Control | App Control Advanced** page. The list of categories is available in the Category drop-down menu.



### To configure an App Control policy for an application category:

1. Navigate to the **POLICY | Rules and Policies > App Control | App Control Advanced** page.
2. Select an application category from the **Category** drop-down menu. The **Configure** icon to the right of the field is enabled as soon as a category is selected.

- Click **Configure** to display the **App Control Category Settings** dialog for the selected category.

- To block applications in this category, select **Enable** in the **Block** drop-down menu.
- To create a log entry when applications in this category are detected, select **Enable** in the **Log** drop-down menu.
- To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
- To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
- To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
- To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
- To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:

### SCHEDULE OPTIONS

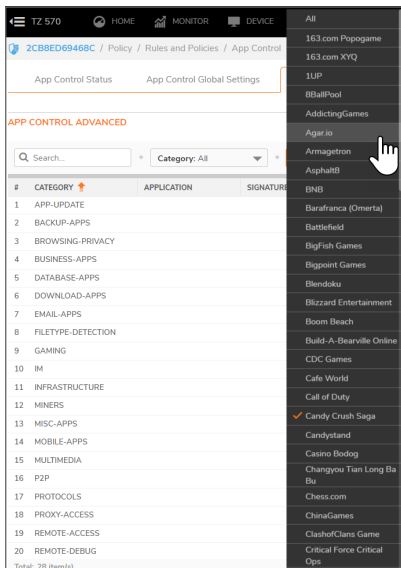
This schedule	Enables the policy
<b>Always on</b>	At all times. This option is selected by default.
<b>Work Hours</b>	Monday through Friday, 8:00 AM to 5:00 PM.
<b>M-T-W-T-F 08:00 to 17:00</b>	Monday through Friday, 8:00 AM to 5:00 PM (same as <b>Work Hours</b> ).
<b>After Hours</b>	Monday through Friday, 5:00 PM to 8:00 AM.
<b>M-T-W-T-F 00:00 to 08:00</b>	Monday through Friday, midnight to 8:00 AM.
<b>M-T-W-T-F 17:00 to 24:00</b>	Monday through Friday, 5:00 PM to midnight.
<b>SU-S 00:00 to 24:00</b>	24 hours a day, Sunday through Saturday (same as <b>Always On</b> ).
<b>Weekend Hours</b>	Friday at 5:00 PM through Monday at 8:00 AM.
<b>AppFlow Report Hours</b>	During the time configured for AppFlow reports.

<b>This schedule</b>	<b>Enables the policy</b>
<b>SU-M-T-W-TH-F-S 00:00 to 24:00</b>	24 hours a day, Sunday through Saturday (same as <b>Always On</b> ).
<b>TSR Report Hours</b>	During the time configured for TSR reports.

11. By default, the **Use Global Settings** option is selected and has a default of **60** seconds, which cannot be changed (the field is dimmed). To specify a different delay between log entries for repetitive events:
  - a. Deselect the **Use Global Settings** checkbox. The field becomes available.
  - b. Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is 0.
12. Click **OK**.

## Configuring App Control Advanced by Application

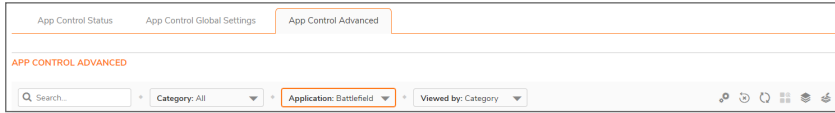
Application-based configuration is the middle level of policy configuration on the **POLICY | Rules and Policies > App Control | Signatures** page, between the category-based and signature-based levels.



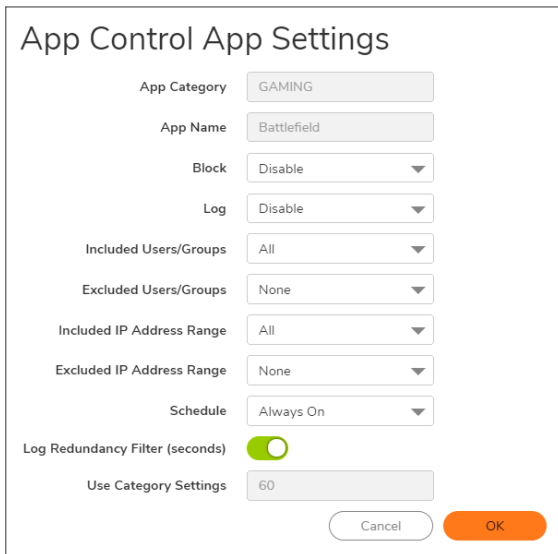
This configuration method allows you to create policy rules specific to a single application if you want to enforce the policy settings only on the signatures of this application without affecting other applications in the same category.

**To configure an App Control policy for a specific application:**

1. Navigate to the **POLICY | Rules and Policies > App Control | App Control Advanced** page.
2. Select an application from the **Application** drop-down menu (if you did not select a category, the category changes to that of the selected application). The **Configure** button to the right of the field is enabled as soon as an application is selected.



3. Click **Configure** to display the **App Control App Settings** dialog for the selected application.



**TIP:** If the application's **Block** setting is set to **Use Category Setting**: To prevent the category settings from overriding your settings for the application, change the **Block** setting here to **Enabled** or **Disabled**, as desired, and update any other settings in this dialog to the specific values that you want.

The fields at the top of the dialog, **App Category** and **App Name**, are not editable. The other settings default to the current settings of the category to which the application belongs. To retain this connection to the category settings for one or more fields, leave this selection in place for those fields.

4. To block this application, select **Enable** in the **Block** drop-down menu.
5. To create a log entry when this application is detected, select **Enable** in the **Log** drop-down menu.
6. To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
7. To exclude a specific user or group of users from the selected block or log actions, select a user group or user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
8. To target the selected block or log actions to a specific IP address or address range, select an **Address Group** or **Address Object** from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

9. To exclude a specific IP address or address range from the selected block or log actions, select an **Address Group** or **Address Object** from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
10. To enable this policy during specific days of the week and hours of the day, select one of the schedules from the **Schedule** drop-down menu. For a list of schedules, see **Schedule Options** in [Configuring App Control Advanced by Category](#).
11. By default, the **Log Redundancy Filter** has the **Use Category Settings** option selected; the field is dimmed and cannot be changed. To specify a different delay between log entries for repetitive events:
  - a. Clear the **Use Global Settings** checkbox. The field becomes available.
  - b. Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is 0.
12. Click **OK**.

## Configuring App Control Advanced by Signature

Signature-based configuration is the most specific level of policy configuration on the **POLICY | Rules and Policies > App Control | App Control Advanced** page.

Setting a policy based on a specific signature allows you to configure policy settings for the individual signature without influence on other signatures of the same application.

### *To configure an App Control policy for a specific signature:*

1. Navigate to the **POLICY | Rules and Policies > App Control | App Control Advanced** page.
2. Select **Signature** in the **Viewed by** drop-down menu.
  - ① **TIP:** Optionally reduce the number of signatures displayed by selecting a category from the **Category** drop-down menu and/or an application from the **Application** drop-down menu.



- ① **TIP:** If you know the Signature ID of the signature, click the **Lookup Signature ID** icon in the toolbar, enter the Signature ID, and then click the **Lookup Signature**.
3. Click **Configure** in the row for the signature you want to work with. The **App Control Signature Settings** dialog displays.

**TIP:** If the signature’s **Block** setting is set to **Use App Setting**. To prevent the application settings from overriding your settings for the signature, change the **Block** setting here to **Enabled** or **Disabled**, as desired, and update any other settings in this dialog to the specific values that you want.

The fields at the top of the dialog are not editable. They display the values for the **Signature Category**, **Signature Name**, **Signature ID**, **Application ID**, **Priority**, and **Direction** of the traffic for the category and application to which this signature belongs.

**TIP:** To edit the application information, click the **Edit** icon next to the **Application ID** field. The **App Control Application Settings** dialog displays. For information about configuring the settings in this dialog, see [Configuring App Control by Application](#).

The other settings for the signature default to the current settings for the application to which the signature belongs. To retain this connection to the application settings for one or more fields, leave this selection in place for those fields.

4. To block this signature, select **Enable** in the **Block** drop-down menu.
5. To create a log entry when this signature is detected, select **Enable** in the **Log** drop-down menu.
6. To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
7. To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
8. To target the selected block or log actions to a specific IP address or address range, select an **Address Group** or **Address Object** from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
9. To exclude a specific IP address or address range from the selected block or log actions, select an **Address Group** or **Address Object** from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
10. To enable this policy during specific days of the week and hours of the day, select one of the schedules from the **Schedule** drop-down menu. For a list of schedules, see [Schedule Options in Configuring App Control Advanced by Category](#).

11. By default, the **Log Redundancy Filter** has the **Use Category Settings** option selected; the field is dimmed and cannot be changed. To specify a different delay between log entries for repetitive events:
  - a. Deselect the **Use Global Settings** checkbox. The field becomes available.
  - b. Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is **0** (no delay), the maximum is **999999**, and the default is **0**.
12. To see detailed information about the signature, click [here](#) in the **Note** at the bottom of the dialog.
13. Click **OK**.

## Viewing Signatures

You can change the **POLICY | Rules and Policies > App Control | Signatures** display through the various **Viewed by** options, which include **Signature**, **Application**, and **Category**.

#	CATEGORY	APPLICATION	SIGNATURE NAME	ID	BLOCK	LOG	DIRECTION	COMMENTS
1	APP-UPDATE	Trend Micro	HTTP Activity 1	216			Outgoing, to Server	
2	APP-UPDATE	Trend Micro	HTTP Activity 2	217			Outgoing, to Server	
3	APP-UPDATE	Microsoft Windows Updates	HTTP User-Agent Industry Update Control	220			Outgoing, to Server	
4	APP-UPDATE	Microsoft Windows Updates	HTTP User-Agent Windows Update Agent	223			Outgoing, to Server	
5	APP-UPDATE	Apple Updates	Software Update 1	299			Outgoing, to Server	
6	APP-UPDATE	WebSense	Security Update	315			Outgoing, to Server	
7	APP-UPDATE	Acesso	InstallAnywhere Update	317			Outgoing, to Server	
8	APP-UPDATE	Oracle Java	Update	327			Outgoing, to Server	
9	APP-UPDATE	Trend Micro	HTTP Activity 3	634			Outgoing, to Server	
10	APP-UPDATE	Ubuntu APT	Update Traffic	782			Outgoing, to Server	
11	APP-UPDATE	BitDefender	Update 1	785			Outgoing, to Server	
12	APP-UPDATE	BitDefender	Update 2	788			Outgoing, to Server	

This View Style	Has this option	Which displays all
<b>Category</b>	<b>All</b> (default)	Categories and their signature applications
	<b>Individual category</b>	Signature applications for the specified category
<b>Application</b>	<b>All</b> (default)	Signature applications associated with the specified category or categories
<b>Viewed by</b>	<b>Signature</b>	Signature applications associated with the specified category and the signatures associated with the application
	<b>Application</b> (default)	Signature applications associated with the specified category or categories
	<b>Category</b>	Categories or the category specified in the Category View Style

You can also display the **App Control Signature Settings** dialog for a particular signature by entering its ID in the **Lookup Signature ID** field after clicking the **Lookup Signature ID** icon.

Click any blue **Application** or **Signature Name** entries to view information on the **App Signature Details** dialog.



## Topics:

- [Viewing by All Categories and All Applications by Applications](#)
- [Viewing by All Categories and All Applications by Signatures](#)
- [Viewing by All Categories and All Applications by Category](#)
- [Viewing Just One Category](#)
- [Viewing just One Application](#)
- [Displaying Details of Signature Applications](#)
- [Displaying Details of Application Signatures](#)

## Viewing by All Categories and All Applications by Applications

For a description of the columns displayed in the **App Control Advanced** table, see [Viewing by All Categories and All Applications by Signatures](#).

The screenshot shows the 'App Control Advanced' view with the following table data:

#	CATEGORY	APPLICATION	SIGNATURE NAME	ID	BLOCK	LOG	DIRECTION	COMMENTS
1	APP-UPDATE	Trend Micro		216				
2	APP-UPDATE	Microsoft Windows Updates		220				
3	APP-UPDATE	Apple Updates		299				
4	APP-UPDATE	WebSense		315				
5	APP-UPDATE	Acresso		317				
6	APP-UPDATE	Oracle Java		327				
7	APP-UPDATE	Ubuntu APT		782				
8	APP-UPDATE	BitDefender		785				
9	APP-UPDATE	AVG		789				
10	APP-UPDATE	Rising Antivirus		790				
11	APP-UPDATE	Avira		792				
12	APP-UPDATE	Firefox Updates		793				

## Viewing by All Categories and All Applications by Signatures

The screenshot shows the 'App Control Advanced' view with the following table data:

#	CATEGORY	APPLICATION	SIGNATURE NAME	ID	BLOCK	LOG	DIRECTION	COMMENTS
1	APP-UPDATE	Trend Micro	HTTP Activity 1	216			Outgoing, to Server	
2	APP-UPDATE	Trend Micro	HTTP Activity 2	217			Outgoing, to Server	
3	APP-UPDATE	Microsoft Windows Updates	HTTP User-Agent Industry Update Control	220			Outgoing, to Server	
4	APP-UPDATE	Microsoft Windows Updates	HTTP User-Agent Windows Update Agent	223			Outgoing, to Server	
5	APP-UPDATE	Apple Updates	Software Update 1	299			Outgoing, to Server	
6	APP-UPDATE	WebSense	Security Update	315			Outgoing, to Server	
7	APP-UPDATE	Acresso	InstallAnywhere Update	317			Outgoing, to Server	
8	APP-UPDATE	Oracle Java	Update	327			Outgoing, to Server	
9	APP-UPDATE	Trend Micro	HTTP Activity 3	634			Outgoing, to Server	
10	APP-UPDATE	Ubuntu APT	Update Traffic	782			Outgoing, to Server	
11	APP-UPDATE	BitDefender	Update 1	785			Outgoing, to Server	
12	APP-UPDATE	BitDefender	Update 2	788			Outgoing, to Server	

<b>Category</b>	Name of the selected signature category or of all signature categories. All signature applications are grouped under the same category heading, such as APP-UPDATE.												
<b>Application</b>	Name of each signature application within a category.												
<b>Name</b>	Signature name.												
<b>ID</b>	Signature ID.												
<b>Block</b>	Indicates whether the category or application is blocked. If blocking is enabled, an <b>Enabled</b> icon appears in this column. The word, <b>Default</b> , might appear for a category.												
<b>Log</b>	Indicates whether the category or application is logged. If logging is enabled, an <b>Enabled</b> icon appears in this column.												
<b>Direction</b>	Traffic direction: <table border="1" style="margin-left: 20px;"> <tr> <td><b>Incoming</b></td> <td><b>Outgoing</b></td> <td><b>Both</b></td> </tr> <tr> <td><b>Incoming, to Client</b></td> <td><b>Outgoing to Client</b></td> <td><b>Both, to Client</b></td> </tr> <tr> <td><b>Incoming, to Server</b></td> <td><b>Outgoing, to Server</b></td> <td><b>Both, to Server</b></td> </tr> <tr> <td><b>Incoming, to Client, to Server</b></td> <td><b>Outgoing, to Client, to Server</b></td> <td><b>Both, to Client, to Server</b></td> </tr> </table>	<b>Incoming</b>	<b>Outgoing</b>	<b>Both</b>	<b>Incoming, to Client</b>	<b>Outgoing to Client</b>	<b>Both, to Client</b>	<b>Incoming, to Server</b>	<b>Outgoing, to Server</b>	<b>Both, to Server</b>	<b>Incoming, to Client, to Server</b>	<b>Outgoing, to Client, to Server</b>	<b>Both, to Client, to Server</b>
<b>Incoming</b>	<b>Outgoing</b>	<b>Both</b>											
<b>Incoming, to Client</b>	<b>Outgoing to Client</b>	<b>Both, to Client</b>											
<b>Incoming, to Server</b>	<b>Outgoing, to Server</b>	<b>Both, to Server</b>											
<b>Incoming, to Client, to Server</b>	<b>Outgoing, to Client, to Server</b>	<b>Both, to Client, to Server</b>											
<b>Comments</b>	This column is blank unless the following has been configured for the category and/or signature application: <ul style="list-style-type: none"> <li>• <b>User</b> icon – User/group inclusion/exclusion settings.</li> <li>• <b>Information</b> icon – IP address inclusion/exclusion settings.</li> <li>• <b>Clock</b> icon – Schedule other than <b>Always On</b>.</li> </ul>												
<b>Configure</b>	<b>Edit</b> icon that displays the appropriate dialog for modifying the signature application settings.												

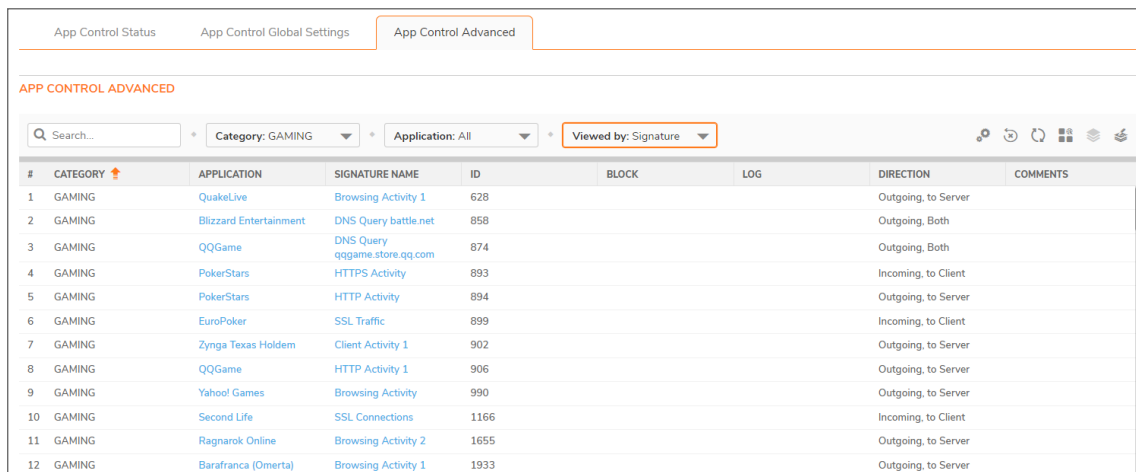
## Viewing by All Categories and All Applications by Category

For a description of the columns displayed in the **App Control Advanced** table, see [Viewing by All Categories and All Applications by Signatures](#).

The screenshot shows the 'App Control Advanced' settings page. At the top, there are three tabs: 'App Control Status', 'App Control Global Settings', and 'App Control Advanced'. Below the tabs, the page title is 'APP CONTROL ADVANCED'. There is a search bar and three filter dropdowns: 'Category: All', 'Application: All', and 'Viewed by: Category'. The 'Viewed by: Category' dropdown is highlighted with a red box. Below the filters is a table with the following columns: #, CATEGORY, APPLICATION, SIGNATURE NAME, ID, BLOCK, LOG, DIRECTION, and COMMENTS. The table contains 12 rows of data, with the first row being 'APP-UPDATE'.

#	CATEGORY	APPLICATION	SIGNATURE NAME	ID	BLOCK	LOG	DIRECTION	COMMENTS
1	APP-UPDATE							
2	BACKUP-APPS							
3	BROWSING-PRIVACY							
4	BUSINESS-APPS							
5	DATABASE-APPS							
6	DOWNLOAD-APPS							
7	EMAIL-APPS							
8	FILETYPE-DETECTION							
9	GAMING							
10	IM							
11	INFRASTRUCTURE							
12	MINERS							

## Viewing Just One Category



The screenshot shows the 'App Control Advanced' tab in the SonicOS 7 Security Services Administration Guide. The interface includes a search bar and filter menus. The 'Category' dropdown is set to 'GAMING', and the 'Application' dropdown is set to 'All'. The 'Viewed by' dropdown is set to 'Signature'. The table below displays 12 rows of data for the 'GAMING' category.

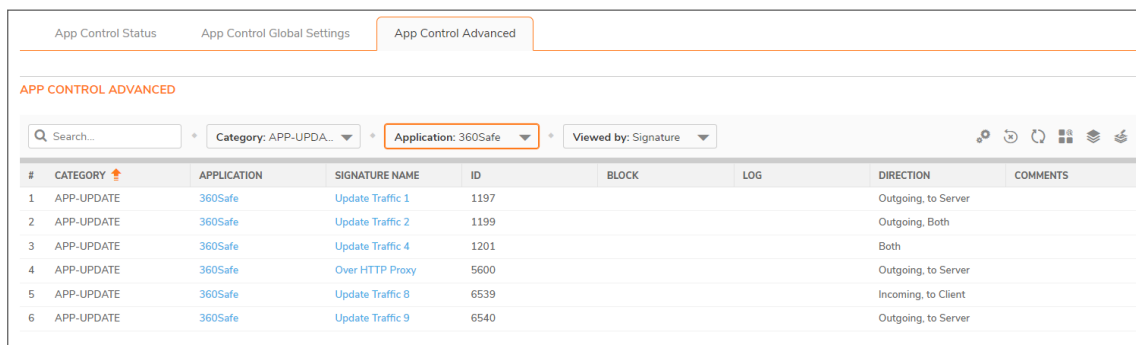
#	CATEGORY	APPLICATION	SIGNATURE NAME	ID	BLOCK	LOG	DIRECTION	COMMENTS
1	GAMING	QuakeLive	Browsing Activity 1	628			Outgoing, to Server	
2	GAMING	Blizzard Entertainment	DNS Query battle.net	858			Outgoing, Both	
3	GAMING	QQGame	DNS Query qqgame.store.qq.com	874			Outgoing, Both	
4	GAMING	PokerStars	HTTPS Activity	893			Incoming, to Client	
5	GAMING	PokerStars	HTTP Activity	894			Outgoing, to Server	
6	GAMING	EuroPoker	SSL Traffic	899			Incoming, to Client	
7	GAMING	Zynga Texas Holdem	Client Activity 1	902			Outgoing, to Server	
8	GAMING	QQGame	HTTP Activity 1	906			Outgoing, to Server	
9	GAMING	Yahoo! Games	Browsing Activity	990			Outgoing, to Server	
10	GAMING	Second Life	SSL Connections	1166			Incoming, to Client	
11	GAMING	Ragnarok Online	Browsing Activity 2	1655			Outgoing, to Server	
12	GAMING	Barafranca (Omerta)	Browsing Activity 1	1933			Outgoing, to Server	

You can restrict the **App Control Advanced** table to display the signature applications of just one category by:

- Selecting a category from the **Category** drop-down menu such as **GAMING** (shown).

## Viewing Just One Application

You can restrict the **App Control Advanced** table to display the signatures of just one application by selecting an application from the **Application** drop-down menu. For a description of the columns displayed in the **App Control Advanced** table, see [Viewing by All Categories and All Applications by Signatures](#).

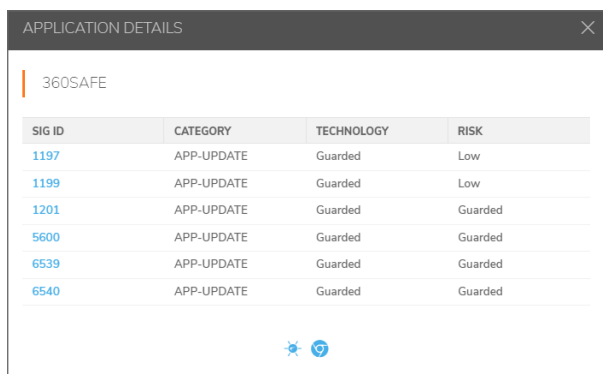


The screenshot shows the 'App Control Advanced' tab in the SonicOS 7 Security Services Administration Guide. The interface includes a search bar and filter menus. The 'Category' dropdown is set to 'APP-UPDA...', and the 'Application' dropdown is set to '360Safe'. The 'Viewed by' dropdown is set to 'Signature'. The table below displays 6 rows of data for the '360Safe' application.

#	CATEGORY	APPLICATION	SIGNATURE NAME	ID	BLOCK	LOG	DIRECTION	COMMENTS
1	APP-UPDATE	360Safe	Update Traffic 1	1197			Outgoing, to Server	
2	APP-UPDATE	360Safe	Update Traffic 2	1199			Outgoing, Both	
3	APP-UPDATE	360Safe	Update Traffic 4	1201			Both	
4	APP-UPDATE	360Safe	Over HTTP Proxy	5600			Outgoing, to Server	
5	APP-UPDATE	360Safe	Update Traffic 8	6539			Incoming, to Client	
6	APP-UPDATE	360Safe	Update Traffic 9	6540			Outgoing, to Server	

# Displaying Details of Signature Applications

You can display details about signature applications by clicking on the (blue) name of the signature application. The Applications Details pop-up dialog displays.



SIG ID	CATEGORY	TECHNOLOGY	RISK
1197	APP-UPDATE	Guarded	Low
1199	APP-UPDATE	Guarded	Low
1201	APP-UPDATE	Guarded	Guarded
5600	APP-UPDATE	Guarded	Guarded
6539	APP-UPDATE	Guarded	Guarded
6540	APP-UPDATE	Guarded	Guarded

<b>Sig ID</b>	Signature ID.
<b>Category</b>	Category of signature application, such as APP-UPDATE, P2P, or GAMING.
<b>Technology</b>	Type of software: <ul style="list-style-type: none"><li>• APPLICATION</li><li>• BROWSER</li><li>• NETWORK INFRASTRUCTURE</li></ul>
<b>Risk</b>	Level of risk for each signature: <ul style="list-style-type: none"><li>• LOW</li><li>• GUARDED</li><li>• ELEVATED</li><li>• HIGH</li><li>• SEVERE</li></ul>

Clicking the signature ID (Sig ID) displays the SonicALERT page for the signature.



**SonicALERT**

Go to [All Categories](#) list.

## 360Safe -- Update Traffic 1

Category: [APP-UPDATE](#)

360Safe is an anti-virus product by Qihoo, an Internet company based in Beijing, PRC.

This SonicWALL signature identifies legitimate 360Safe Update traffic. The primary purpose of this signature is for bandwidth management when used in the Application Firewall feature.

**Virus Advisory**

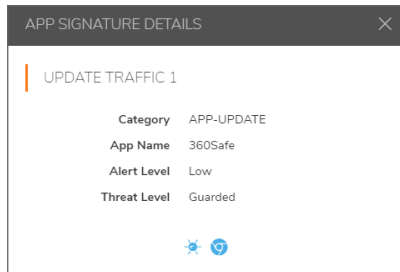
IPS Alert Level

Low Medium High

© SonicWall 2017 | [Privacy Policy](#) | [Conditions for use](#) | Version: 8.1

## Displaying Details of Application Signatures

You can display details about signature applications by clicking on the blue **Signature Name**. The **App Signature Details** pop-up dialog displays.



<b>Category</b>	Category of signature application, such as <b>APP-UPDATE</b> or <b>GAMING</b> .
<b>App Name</b>	Name of the signature application.
<b>Alert Level</b>	Alert level: <ul style="list-style-type: none"><li>• <b>Low</b></li><li>• <b>Medium</b></li><li>• <b>High</b></li></ul>
<b>Threat Level</b>	Level of threat of the signature: <ul style="list-style-type: none"><li>• <b>Low</b></li><li>• <b>Guarded</b></li><li>• <b>Elevated</b></li><li>• <b>HIGH</b></li><li>• <b>SEVERE</b></li></ul>

# 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 Security Services Administration Guide

Updated - January 2021

Software Version - 7

232-005345-10 Rev C

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